2026 International Conference on Cybersecurity, Digital Forensics, and AI Applications (ICCSDFAI 2026)

Istanbul, Turkiye
25-27 June 2026

Pages 1–688

IEEE Catalog Number: CFP263CM-POD
ISBN: 979-8-3195-2049-4

Copyright © 2026, IEEE

All Rights Reserved

Copyright and Reprint Permissions:

Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

*** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.

IEEE Catalog Number:	CFP263CM-POD
ISBN (Print-On-Demand):	979-8-3195-2049-4
ISBN (Online):	979-8-3195-2048-7

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA

Phone:	(845) 758-0400
Fax:	(845) 758-2633
E-mail:	curran@proceedings.com
Web:	www.proceedings.com

CURRAN ASSOCIATES INC. proceedings .com

TABLE OF CONTENTS

Federated Learning–Enhanced SIEM for Multi-SOC Collaboration: Toward Intelligent, Privacy-Preserving Cyber Defense 73
Saloua Walehiane, Mohamed Errais

Penetration Testing Framework Based on Large Language Models: Architecture, Implementation, and Experimental Evaluation 79
Amir Bekbauov, Laura Aldasheva, Maksat Serikuly, Akzhibek Amirova, Dana Tolegen, Askhar Mussa

Development of an Application for Effective Ransomware Detection and Mitigation 84
Moldir Azim, Kymbat Seilkhanova, Dana Tolegen, Dauren Sagidullauly, Aibolat Kurakbayev, Syrym Sapash

Developing a Framework for Analysis of WPA3 and Router Attacks 88
Aitolkyn Kulmuratova, Balziya Aldosh, Syrym Sapash, Kymbat Seilkhanova, Kuanysh Syzdykbayev Laura Kulbayeva

Optical Frequency Comb Generation Using SOA and Two Laser Sources For 6G Signals 94
Yazan Alkhlefat, Sevia M Idrus, Farabi Iqbal

File Carving with Binary Fragment Alignment: An Adjacency Matrix Optimization Approach 100
Yerassyl Yermekov, Madi Shayakhmetov, Kakim Sagyndykov, Abilkair Imanberdi, Aina Tazhiyeva Aliya Zhetpisbayeva

Intelligent Multi Broker Slice as a Service Architecture for Cross Domain Mobility Continuity in 6G Networks 106
Masnaoui Hamza, Pr. Errais Mohammed

AI for Cyber Defense: A Balanced View of Advantages and Security Threats 113
Anar Yessengeldina, Ruslan Tormosov, Daulet Dushabayev, Alisher Batkuldin, Dinara Akimova Karakat Syratay

A Multi-Source Event Correlation Framework for IAM Security Using Machine Learning and Zero Trust Principles 118
Md. Mushfiqur Rahman, Nurmamatov Mekhriddin, Aswani Kumar Cherukuri, Sazzad Hossain

Sensitive Content Screening for Secure Antibiogram Image Sharing in Healthcare AI Workflows 126
Aya Khirania, Mohammed Reda Chbihi Louhdi, Mohamed El Moufid, Yassine Zahidi, Hicham Medromi

Design and Evaluation of an AI-Based Journaling and Emotional Support Prototype 132
Altair Aitymov, Alisher Kulatayev, Baktiar Baibolatov, Kydyrbekova Aigerim

Behavior-Based Risk Scoring for Adaptive CAPTCHA: Design and Preliminary Evaluation 138
Nurmakhan Bakytnur, Maxutova Danelya, Aigerim Kydyrbekova

An AI-Based Face Recognition Approach for Student Attendance: A Prototype System 145
Dias Abdylhalyk, Sayanbek Zhuma, Yernar Aubakir, Aigerim Kydyrbekova

Towards Explainable Intrusion Detection Systems: Improving Trust in AI-based Cybersecurity Models 151
Zarina Daniyarova, Olzhas Konakbayev, Akzhan Beisenova, Zhaiyk Kundaulet, Ayanat Galymzhan

Machine Learning and Deep Learning Approaches for Cyberattack Anomaly Detection: A Concise Review 156
Fares A. Dael, Ibraheem Shayea, Jibran K. Yousafzai

Title: Cybersecurity Resilience in SmartCities: A Critical Analysis of IoT Protocols 162
Youssef Elmnisri, Laila Fetjah

CNN-Based Automatic Modulation Classification on the RadioML2016.10a Dataset 168
Erol Tetik, Ibraheem Shayea, Leila Rzayeva, Perizat Tazhibayeva

Arabic Datasets for Online Child Safety: A Systematic Review 174
Omar Rhouzali, Laila Fetjah, Mohamed Errais

Prompt Injection Through Operational Data Feeds: A Structural Governance Gap in OT-Connected Agentic AI Systems 180
Suhail Ahmad Rana, Dinara Kozhamzharova

Generative AI Governance and Cybersecurity Risk Control in Organizational Development 185
Bin Xu, Zhanibekova Gaukhar

Design and Parametric Investigation of a Wideband FR-4 Microstrip Power Divider 190
Mehmet Onur Kok, Anes Kokorović, Caner Timucin, Şehabeddin Taha İmeci e

Machine Learning-Based Traffic Analysis and Anomaly Detection in Software-Defined Enterprise Networks 193
Alim Kutzhanov, Ibraheem Shayea, Abdulraqeb Alhammadi, Jibran K. Yousafzai

Mobile Agent approach to search for distributed information using fuzzy logic set 199
Ammar Al-Shami, Ibraheem Shayea, Zool Hilmi Ismail, Abdulaziz Alashbi

Federated Learning for Privacy-Preserving Fatigue Detection from Wearable IMU Data 206
Kenza Issellay, Aya Khirania, Safae Elhir, Hicham Medromi

Toward Robust Audio Deepfake Detection in Real Acoustic Environments: Limitations of MFCC-Based Classical Models and the Advantages of Deep Learning with Domain Adaptation 212
Mukhamedali Daniyaruly, Assel Smaiyl, Akzharkyn Zholmyrza

Near-Field Beamfocusing for Large-Array Vehicular ISAC 216
Reham Hatash, Ahmed Al Hilli, Wasan Kadhim Saad

AI-Augmented Career Advising in Universities: Digital Ethics and Security concerns 221
Nurdana Kaiyrgali, Margarita Serebrennikova, Medet Mukushev

Deep Learning for Mobility Management in Next-Generation Wireless Networks: Models, Applications, and Challenges 227
Fares A. Dael, Ibraheem Shayea, Laura Aldasheva, Akzhibek Amirova, Didar Yedilkhan

Development of Intelligent Methods to Enhance VPN Security: Literature review 234
Kanatova Aliya, Zhetessova Gulnara, Moldir Ashimova, Maral Ospanova, Aldasheva Laura

Truncated Quantile Critics for Obstacle-Dense Quadrotor Navigation: A Comparative Study with SAC 238
Zarina Kutpanova, Svitlana Biloshchytska, Abylkhan Khambarov, Almas Dossymbekov

Structural Adaptation Risk in AI-Enabled Security Systems: Framework for Architecture-Centric Control 243
Sinchev Askar, Sinchev Bakhtgerey, Chinchalinova Aigul, Tuleushin Kanysh, Mun Dmitriy, Ospanova Aliya

Low-Cost Honeypot Data for High-Stakes DDoS Detection: Benchmark Inflation vs Real-World Performance 249
Abdulqudos Y. Alnahari, Noor Azurati Ahmad, Essa A. Hizzam

Utilizing 5G Networks to Improve Latency and Connectivity for IoT Devices in Smart Homes 255
Zhansha Ansagan, Bilal Saoud, Didar Yedilkhan, Akhmet Tussupov, Moldir Azim

Autonomous Desert Border Surveillance: Recent Advances in Small Object Detection and Model Compression 262
Mohammed A. Ezzaldeen, Abdulaziz A. Alashbi, Abdulqader M. Mohsen, Ali Ali Farhan

Comparative Performance Evaluation of PV, Wind, and Hydro Systems for Standalone Applications 270
Bappaditta Saha Chowdhury, Md Shahin Alam

Algorithmic Aircraft Accident Analysis Using Machine Learning Models for Predictive Risk Management 276
John Olalere Ogunlola, Olayinka Anthony Ojo, Opeyemi Victor Omolade, Ogechi Smart Ekejiuba Babatunde Alexander Abiola, Bartholomew Sunday Alfred

AI-driven multi-objective optimization of municipal production systems using genetic algorithms 284
Vagif Gasimov, Nizami Jafarov, Jabir Mammadov, Sevinj Aliyeva, Ilhami Suleymanov

Comparative Analysis of Machine Learning and Deep Learning Models for Classification and Regression Tasks in Supply Chain Data 293
Atalay Tural, Bilal Saoud, Ibraheem Shayea, Abdulraqeb Alhammadi, Jibran K. Yousafzai

Security Assessment and Design of a Wireless IoT-Based Programmable LED Display System 298
Syrym Sapash, Batyrkhan Aliyev, Bekarys Sapash, Dauren Sagidullauly, Laura Aldasheva, Darkan Serik

An Integrated Machine Learning and Agent-Based Modelling Pipeline for Socio-Environmental Forecasting 303
Ogechi Smart Ekejiuba, Olayinka Anthony Ojo, Ogunlola John Olalere, Blessing Alice Alao-Olatunji Negin Aboutorabi

Standard Security System Architecture in Society 5.0: Integrated Defense Framework 310
Najaf Mammadzada, Jabir Mammadov, Esmira Mustafayeva, Nizami Jafarov, Kamale Aliyeva

Adaptive AI Powered Intrusion Detection System With Optimized SQL Injection Classification 316
Anuar Askarov, Ibraheem Shayea, Abdulraqeb Alhammadi, Jibran K. Yousafzai, Samat Mukhanov

An Ensemble-Based Deep Learning Framework for Automated Diabetic Retinopathy Grading from Retinal Fundus Images 322
Zahra Esparghami, Mohammadparsa Malek, Ozan Duru, Sena Serefoglu

Software Module for Frame Extraction and Generation of Video Clips with People from Long Video Recordings 328
Timur Grigoryev, Alisher Batkuldin, Murat Zhakenov, Denis Davydov, Kuandyk Niyazaliev Zhankulov Daniyar

Video stream interception of IoT system 334
Saken Tleuberdin, Konstantin Malakhov, Aliya Issainova, Dina Satybaldina, Nurlan Tashatov

Solar Power Generation Forecasting Using Historical Weather Data and Machine Learning Techniques 338
Nijat Muhammed, Fares A. Dael, Ibraheem Shayea, Abdulraqeb Alhammadi, Jibran K. Yousafzai

Cyber Threat Risk Assessment from Hacker Forum Emotion and Activity Signals 344
Saken Mambetov, Askar Khikmetov, Serik Joldasbayev, Bakhytzhan Kulambayev, Kuanysh Dossanbek Tolganay Chinibayeva

Forensic Data Extraction and Recovery from Unmanned Aerial Vehicles: A~Framework for DJI-Based Platforms 352
Yerassyl Yermekov, Madi Shayakhmetov, Denis Davydov, Leila Rzayeva, Azamat Baibussinov Dias Yessenov

Comparative Analysis of CNN-TDNN and CNN-LSTM Architectures for Voice Activity Detection under Low Signal-to-Noise Ratio Conditions 358
Aigul Kulakayeva, Aigul Nurlankyzy, Bagdat Kozhakhmetova

A Systematic Evaluation of Feature Reduction and Hybrid Sampling Strategies for 5G-NIDD 363
Humam Ali Hameed, Sarmad Khalil Ibrahim

A Systematic Review of Load Forecasting and Energy Management Studies in Electrical Power Systems 369
Korhan Kayisli, Ruhi Zafer Caglayan, Leila Rzayeva, Fatih Gundogdu

Energy-Efficient UAV Trajectory Planning for Water Quality Monitoring Using a Hybrid NN–2Opt Approach 376
Mohammad Alnakhli, Abdullah Nihad, Bader Fayez, Ahmed Abdullatif, Hadhal Ayed, Faris Abdullah

Machine-Learning-Aided Screening of Heat-Network Renewal Pressure in Kazakhstan's CHP-Linked Power System during the Green-Economy Transition 382
Dongli Liu, Gulashar Z. Doskeyeva, Zhazira Kusmoldayeva

Comparative Evaluation of Speaker Diarization Models on Kazakh-Russian Mixed Audio Dataset 387
Amirkhan Ilyassov, Nursultan Nyssanov, Leila Rzayeva, Kuandyk Niyazaliev, Akan Baltabayev Azamat Baibussinov

Robust Hybrid Image Steganography with Reed-Solomon Error Correction for JPEG-Resilient Covert Communication on Messaging Platforms 393
Vladislav Khegay, Balziya Aldosh, Rostyslav Lisnevskyi, Vitalii Lisnevskyi, Askar Syssoyev Batyrkhan Aliyev

Long-term Social Engineering in Corporate Environments: Dedicated Risk Assessment Tool 399
Vladislav Khegay, Nursulu Belessova, Assel Issakhanova

Machine Learning-Based Early Detection of Chaos and Cyber Threats in Economic Dynamics 405
Beisenbi Mamyrbek, Didar Yarulin

A Multi-Class Supervised Neural Network Framework for Cyber Threat Classification in Telecommunications Traffic 411
Aidar Ispussinov, Arstan Makatov, Ruslan Omirgaliyev, Gaukhar Yerzhigitova, Aruzhan Abdulina

Digital Transformation of the Educational Process at UWED: The Experience of Implementing an Integrated System for Managing Academic Activities 417
Muzaffar Djalalov, Shakhnoza Teshaeva

Digital Twin Orchestration in Transnational Energy Corridors 425
Muzaffar Djalalov, Dilshoda Juraboeva

Wallet verification methods in blockchain applications 432
Adilet Ormanov, Dastan Bekesh, Valeriy Fedorenko, Zhaksylyk Kozhakhmet, Nadezhda Nikiforova, Li Yin

Metaheuristic Framework for SQL Injection Vulnerability Testing 437
Fakhreldin Ali, Ashraf Osman Ibrahim, Maged Nasser, Mohammad Ahsanul Islam, Saule Amanzholova Damelya Yeskendirova

Machine Learning-Based Assessment of Hydropower Integration and Regional Net Exchange in East Kazakhstan 443
Altynshash Rakhimzhanova, Aiganym Mansurova, Nurkhat Zhakiyev

Building an Information Model for the Construction Site Selection Problem 449
Elena Gorda, Yuliia Kroshka, Nadiia Martyniuk

Blockchain and the Internet of Things in Military Infocommunication Systems: Selecting a Consensus Mechanism Based on Multi-Criteria Analysis 455
Ruslan Ospanov, Yerzhan Seitkulov, Banu Yergaliyeva, Nurlan Tashatov, Kuat Utebayev, Serik Zhuzbayev

UNIBANK STATEMENT INTEL: An Intelligent System for Universal Bank Statement Processing and Financial Transaction Categorization Using Large Language Models 461
Askar Khikmetov, Azamat Kaliyev, Alem Ibrayeva, Gaini Mukhanova, Zhaksylyk Kozhakhmet Aina Tazhiyeva

Intelligent Air Route Optimisation for UK Domestic Aviation Through Machine Learning-Based Passenger Demand and Load Factor Analytics 467
John Ogunlola, Christiana Olalere, Dan Taiye Aremu, Blessing Alao-Olatunji, Oluwakemi Onabolu Opeyemi Victor Omolade

Towards Augmented Security Operations Centers: A Cognitive State-Aware Approach for Proactive Analyst Fatigue Monitoring 474
Anas Sayah, Imane Lotfi, Meriem Mandar

ML-Driven Automated Response Policy Engine for Cyberattack Prevention in SOC: From Detection to Action Decision 480
Imane Lotfi, Anas Sayah, Meriem Mandar

Hybrid STSMC Observer and AI-Based Anomaly Detection in Smart Grids with EV Integration 486
Korhan Kayisli, Ruhi Zafer Caglayan, Erdal Irmak, Leila Ryzayeva, Ahmet Gundogdu

Ontology-Based Enhancement of IoT Logs for Digital Forensic Investigations A Controlled Experiment with Smart Lock Data 493
Ahmed Abdulla Almarzooqi, Mihai Boicu

An analytical review of cybersecurity vulnerabilities and AI-based protection in EV charging systems 499
İzviye Fatımanur Tepe, Oğuz Taşdemir, Korhan Kayisli, Erdal Irmak

Cyber–Physical Security Challenges in Hybrid Energy Storage for Renewable–EV Microgrids 506
Bappaditta Saha Chowdhury, Md Shahin Alam, Shahed Enamul Quadir

Quantum Optimization for Finance: Algorithms, Hybrid Pipelines, and the State of Practical Advantage in the NISQ Era 512
Batuhan Hangun, Oguz Altun, Onder Eyecioglu, Korhan Kayisli, Murat Beken

An Optimized DenseNet-121 Framework for Highly Sensitive and Interpretable Pneumonia Detection from Chest X-Rays 517
Erol Akif Kurtcebe, Kubilay Ayturan, Firat Hardalac, Erdem Yanar

Coordinated Operation of Data Center Aggregations in Modern Distribution Networks 522
Isaac Papa Kwesi Arkorful, Charles Ofori, Margaret Boateng, Prince Asiamah Addo
Yaw Amankrah Sam-Okyere, Edmund Azundow Dasori

Sustainable Operation of Data Centers: Energy Consumption Modeling and Reduction Approaches 528
Wisdom Elipklim Korkortsi, Charles Ofori, Prince Asiamah Addo, Margaret Boateng, Gloria Opoku Darkoh
Isaac Papa Kwesi Arkorful

Random Forest Regression for Energy Forecasting in Hybrid Solar-Wind Systems 534
Kofi Kwaasi Asare, Florence Dela Kpodo, Wisdom Elikplim Korkortsi, Samuel Kafui Kwawukume
Charles Ofori, Martin Luther King

Predicting Particulate Matter 2.5 Concentration in Beijing Using Weather and Pollution Indicators With Machine Learning 540
Gökay Ata Sır, Ibraheem Shayea, Samat Kairambayev, Assel Nurgizhina, Vitalii Lisnevskyi

Secure Coding Practices in Modern Web Frameworks: An Empirical CVE-Based Analysis and Comparative Security Evaluation 547
Laura Aldasheva, Alua Tanirbergenova, Timur Satymbayev, Zaure Yanabaeva, Sanida Yessenbek
Yertay Daulet

Anomaly Based Zero-Day Attack Detection in IoT Systems with Honeypot Based Data 551
Cerennur Korkut, Ceyda Kahraman, Burak Çağrı Aydin, Murat Beken

ECG Derived Respiratory With AM Modulation 555
Mehmet Feyzi Aksahin, Mehmet Karademir

Personalized Federated Learning Systems for Secure and Private Analysis of Patient Medical Records 560
Adil Akhmetov, Bauyrzhan Berlikozha, Maxat Amreyev, Farikha Nauruzbayeva

Centralized and Decentralized Energy Management Controls for Microgrids: Architectures and Open Challenges 566
Emmanuel Wiafe, Charles Ofori, Margaret Boateng, Prince Asiamah Addo, Martin Luther King
Lambert Dwomoh

Application of Artificial Intelligence Methods in Radiation Risk Assessment and Decision Support for Civil Protection Systems 572
Syrym Sharipkhanov

Interpretable Artificial Intelligence Models Based on Large Language Models for Web Application Vulnerability Detection and Security Analysis 578
Ilya Shelestov, Aliya Kanatova, Neilya Yessentay, Gulnara Zhetessova

LLM Generated Turkish Email Dataset and Phishing Detection Benchmark 586
Melike Akdağ, Aliye Yeşim Yaman, Özgü Özkan, Nesil Bor, Nergis Pervan Akman

Weather Forecasting with Deep Kalman Filter 592
Ibrahim Kocak, Ibraheem Shayea, Aizhan Omarova, Murat Zhakenov

Transfer Learning for Landmark Recognition and Geographic Localization in Smart City Environments 599
Adilbek Bisenbaev, Bekarys Nurzhauabev, Nursultan Nyssanov, Daniyar Zhankulov, Meiir Raikhan Alibek Bektaev

A Deep Learning-Based Malware Triage Framework with Uncertainty-Aware Detection for SOC Environments 604
Aymane Mossadaq, Meriem Mandar

Modeling and analysis of risks in IT projects using mathematical methods: Bayesian Networks and Monte Carlo Simulation 609
Gulshat Khamidulla, Aivar Sakhipov, Riza Akhitova, Almira Kulmaganbetova, Zhanat Babazhanova Zhanbai Uzdenbayev

Digital Twin and IoT Based Intelligent Library Navigation and Localization System 615
Sachit Sharma, Jetendra Joshi, Vinay Kainthola

Software Defense Against Reverse Engineering Using a Hardware-Bound Split-Key Framework 620
Ali Myrzatay, Gul Jussupova, Daniyar Zhankulov, Zhaksylyk Kozhakhmet, Alissa Ryzhova Alisher Batkuldin

A Self-Organizing Control System for a Nonlinear Spacecraft under Cyber-Physical Uncertainties in the Disaster Class Hyperbolic Umbilic 627
Mamyrbek Beisenbi, Orisbay Abdiramanov, Nauryz Kanysh, Lyudmila Soboleva, Akerke Auyelbayeva Darkan Serik

Development of an Analytical and Applied Project Management Model for Kazakhstan's Event Industry in the Context of Digital Transformation 639
Aruzhan Abdybayeva, Gaini Mukhanova, Aikun Akhmetzhanova, Anar Yessengeldina, Dilnaz Iskakova Merey Shakenova

Evaluating AI Implementation in Government Agencies: A Project Management Approach 645
Gaini Mukhanova, Aruzhan Abdybayeva, Aikun Akhmetzhanova, Aigul Kosherbayeva, Anar Yessengeldina Arzu Assylbekova

Improving Project Management Efficiency in Financial Intelligence Systems through Low-Code RPA 650
Aruzhan Abdybayeva, Diana Imambekova, Gaini Mukhanova, Aikun Akhmetzhanova, Nadezda Rogaleva Anar Yessengeldina

Data Analytics in Banking: Improving Financial Monitoring and Risk Control 656
Gaini Mukhanova, Aikun Akhmetzhanova, Aruzhan Abdybayeva, Meruyert Abildina, Anar Yessengeldina Moldir Kabdygaliyeva

Using PRINCE2 in the Development of Financial Monitoring Systems 662
Anar Yessengeldina, Aikun Akhmetzhanova, Yerzhan Khalbayev, Gaini Mukhanova, Ayazhan Zhaksylyk Zhanar Taizhanova

Financial Risk Management of Secure Digital Twins in Critical Infrastructure: A Resilience-Oriented Framework for Investment and Operational Decision-Making 667
Zhu Yuanyuan, Irina S. Karabulatova, Olga Ergunova, Andrey G. Somov, Elena G. Kiseleva Gaini Mukhanova

AI-Driven Financial Decision Support in Digital Twin Ecosystems for Critical Infrastructure: Lifecycle Cost Optimization and Risk-Aware Management 672
Pooja Kansra, Gaini Mukhanova, Olga Ergunova, Evgeny Makarenko, Anupriya Sharma Ghai Marina Morozova

Integrated FinTech and Digital Twin Methodology for Risk Management in AI-Enabled Cyber-Physical Systems 678
Inga Skvortsova, Gaini Mukhanova, Sergey Chayuk, Andrey G. Somov, Irina Bagaeva, Aleksey Fadeev

Human-Centric and AI-Augmented Financial Risk Management in Secure Digital Twin Ecosystems for Critical Infrastructure 683
Olga Ergunova, Andrey G. Somov, Stas Konovalov, Gaini Mukhanova, Natalia Belyakova, Pawan Kumar

Generative Deep Learning Framework for Restoring Damaged Digital Evidence: Prototype for Image Inpainting 689
Vladislav Khegay, Shyryn Tutkyshbayeva, Gulnur Shuteyeva, Ainur Tokzhigitova

Preventing school cyberbullying through detection of photo and video materials: design and evaluation blueprint for a privacy-preserving multimedia detector 695
Rabiga Suleimenova, Kyrmyzy Zhumabekova, Nursulu Algozhaeva

An Intelligent Workflow Platform with AI-Based User Activity Analysis and Security Monitoring 702
Shynar Yelezhanova, Ayan Kemel, Dametken Baigozhanova, Aivar Sakhipov, Yersultan Tulebayev Nurzhan Ualiyev

Preparing educators for innovative activities in the context of digitalization and AI implementation 708
Suleimenova Rabiga, Syzdykova Zuleikha, Salykova Leila, Abylkassova Arailym

Methods for Evaluating the Influence of Artificial Intelligence on Project Decision-Making 714
Aikun Akhmetzhanova, Gamzat Mamash, Aruzhan Abdybayeva, Adelya Sarmanova, Gaini Mukhanova Anar Yessengeldina

Experimental Setup of a Hydrogen-Based Microgrid: Design and Implementation of a Small-Scale Prototype 718
Khaled Alzaareer, Mohammad Khirfan, Baraa Alswaeer, Ruba Qutaish, Batool Alsawair, Baraa Razmeh

Digital Twins as an Integrative Platform for Energy Efficiency, Renewable Integration and Global Competitiveness of Energy Companies: A Conceptual Synthesis 724
Olga Ergunova, Inga Skvortsova, Andrey G. Somov, Sergey Chayuk, Svetlana Dusenko, Gaini Mukhanova

Towards Sustainable Drone Flight Planning using Neuromorphic Computing 729
Roumaissa Lallouche, Ahmed Alioua, Mohamed Nadjib Zennir, Amine Bouderbala

Privacy-Preserving Identity and Entitlement APIs for External Ecosystems 735
Nithesh Gudipuri

AI-Powered Anomaly Detection in Public Procurement Using NLP and Structural Analysis of Kazakh Government Contracts 741
Fakhreddin Khasanov, Nursultan Nyssanov, Nazgul Ibrayeva, Anor Mukasheva, Alisher Ibrayev Arailym Orazova

AID-ZT4B5G: an Adaptive Intelligent Zero-Trust Multi-Layer Architecture for B5G Networks 749
Ishaq Amimour, Ahmed Alioua, Aboubakr Chettab

Development and Cybersecurity Evaluation of an AI-Based Clinical Decision Support Portal for Blood Gas Analysis and Secure Patient Data Management 756
Indira Uvaliyeva, David Borozenets, Zhenisgul Rakhmetullina, Zharas Nurumov

Monitoring and Control of a Small-Scale Hydrogen-Based Microgrid 764
Khaled Alzaareer, Baraa Razmeh, Baraa Alswaeer, Mohammad Khirfan, Ruba Qutaish, Batool Alsawair

QFLARE: A Post-Quantum Federated Learning Framework with Cryptographically Enforced Privacy and Byzantine Resilience 770
Aditya Patel

StrideDS: A Hybrid Host–Network Dataset for Intrusion Detection in Smart Home IoT 776
Shahbaz Ali Imran, Junaid Arshad, Yussuf Ahmed, Fuad A. Ghaleb

A Hybrid Dual-Backbone Deep Learning Framework for Lumbar Spinal Stenosis Classification from MRI with External Validation 784
Sadia Hamid, Mugdha Farheen Kibria, Fatema Tuz Zohora Panna, Marjana Khanam Roza Mansura Afsana Rima, MD Rezaul Karim, Tauhidur Rahman Sakib

An Early Warning System for Systemic Cyber Risk in Banking Sectors Using Machine Learning and Network Analytics 790
Adejor E. Abiche, Leila Rzayeva, Mohamed A. Hamada

Advancing Health Care Informatics Through You Only Look Once v10 for Lung Nodule and Cancer Detection in Medical Imaging Systems 797
Mohammad Tubishat, Ahed Abugabah, Ahmad Mohammad Al-Smadi

Preserving Forensic Indicators in Mobile Text Preprocessing: An Android 15 Case Study 803
Rahib Aghababayev, Yadigar Imamverdiyev

A Blockchain-based Integrity Layer for Android Forensic Chain-of-Custody Verification 809
Dariga Abduali, Dayana Rakhmatullina, Leila Rzayeva, Mohamed Ragab, Elvira Alimova

SHIELD: Safety-Oriented Class Balancing via Protocol-Aware Missingness for Multi-Class Anomaly Detection in Industrial Control Systems 816
Md Baharul Islam, Jabed Hasan Tarek, Mohammad Shah Paran, Abdul Hasib

Vulnerability-Seeded Code Synthesis for Benchmarking Static Analysis Security Tools 824
Afsar Khan

AI-Based Digital Security Management System for Schoolchildren: Architecture, Detection Models, and Real-Time Intervention 830
Sultanova Elmira, Sultanova Gulzhazira, Saule Dostanbayeva, Asaumurzina Gulnaz, Zhanar Zhampeisova Alua Kossemova

Development of a New Method for a VPN Configuration Platform for Corporate Networks 837
Sagynbayeva Aitolkyn, Vladislav Khan, Askhat Takayev, Aliya Zhetpisbayeva

Transformer-Based Semantic Similarity Detection for Cross-Device Text Forensics 844
Dayana Rakhmatullina, Dariga Abduali, Mohamed Ragab, Amina Almagambetova, Leila Rzayeva

QR Security Checker: A Mobile Framework for Detecting Illicit Content Behind QR Codes and Its Alignment with International Cybercrime Law 850
Aidar Saitbekov, Madi Shayakhmetov, Dana Kaskabayeva, Kuantay Saginayev, Perizat Tazhibayeva

Bilingual End-to-End Neural Diarization for Kazakh-Russian Code-Switched Speech 856
Amirkhan Ilyassov, Zuleikha Syzdykova, Serik Igbayev, Khikmetov Askar, Denis Davydov, Gerald Feldman

Bring Your Own Encryption (BYOE) in Government and Enterprise Systems: Architecture, Benefits, and Challenges 862
Nurbekkyzy Dana, Atanbayev Yernat, Kabdylkak Arnur, Sailau kyzy Zhuldyz, Satybaldina Dina

A Robust Hardware-Software Method for Bit-Stream Image Acquisition from Physically Damaged Flash Memory Modules in Civilian UAVs 868
Azamat Baibussinov, Alina Belonossova, Gulnara Abitova, Kaisarbek Yesbergenov, Daulet Toibazarov Yermek Zhapelov

Deep Multi-Modal Learning for Automated Categorization and Evidence Triaging in Large-Scale Drone Forensic Archives 874
Azamat Baibussinov, Aliya Ospanova, Gulnara Abitova, Kaisarbek Yesbergenov, Ibraheem Shayea Aina Tazhiyeva

Self-Reflective LLM Agents with Quality-Aware Episodic Memory for Multi-Step Task Completion 882
Balaji Narasimhalu Mohanam

Verifier-Guided Autonomous SQL Generation Using LLM Agents and Schema-Aware Retrieval 888
Balaji Narasimhalu Mohanam

AI-Assisted Regulatory Compliance in Electronics Manufacturing: Comparative Analysis of Government Approaches 894
Anara Tasbolat, Igor Seniushin, Yernat Atanbayev, Natalya Glazyrina, Uvalieva Indira

NotPetya: Anatomy of a Cyberweapon Disguised as Ransomware 900
Yerassyl Yermekov, Zamir Khailudayev, Dariga Kudaibergen, Ramazan Khairullin, Karima Zhunis

AI-Driven Penetration Testing: A Survey of Autonomous Agents, LLM-Based Approaches, and Future Directions 904
Kamalbek Berkimbayev, Gulnara Abitova, Auelbek Perizat, Ramazan Khairullin, Karima Zhunis Dariga Kudaibergen

Evaluating Password Security Habits and Cybersecurity Awareness Among Students of Astana IT University: A Quantitative Case Study 911
Aidar Ispussinov, Abylaikhan Baktykeriev, Azamat Tleukhan

A Dual-Layer Security Framework for Healthcare Data Protection Using Blockchain and Machine Learning 917
Alissa Ryzhova, Gul Jussupova, Daniyar Zhankulov, Pavel Kim, Baktiyar Toksanbay, Ali Myrzatay

Explainable Deep Learning for Behavioral Malware Classification: An Attention-Based Analysis of API Call Sequences 924
Soltanbay Kunnur, Shegebay Arsen, Sabituly Dinmukhamed, Bakgeldi Alkhabay

Adaptive AI Malware: The Rise of Self-Evolving Threats That Learn to Evade Defenses 930
Maksat Meshituly, Yerali Dossybekov, Zhumadilov Timur, Aisagaliyev Islam, Meiirgali Mussylmanbay Batyrkhan Aliyev

Ransomware Attacks and Their Impact on Organizations: Evolution, Patterns, and Mitigation Strategies 935
Natalya Glazyrina, Daniyar Kamalov, Sanat Sadu, Aruzhan Yessilbekova, Rashitdin Kokenov

The Role of Online Anonymity in Cyberbullying Behavior on Social Media Platforms 940
Aidar Ispussinov, Ibragim Satbekov, Doskhan Dosmaganbet, Nurkhat Sagyngali

Securing the Physical-Digital Frontier: AI for Anomaly Detection in OT, IoT, and Critical Infrastructure 945
Kozhanazarov Zamir, Yerali Dossybekov, Zhumadilov Timur, Ilhami Colak, Erdal Irmak, Korhan Kayisli

AI-Powered Phishing Attacks and How to Prevent Them: A Comprehensive Survey and Framework 950
Dashoev Sultan, Daniyar Kamalov, Sanat Sadu, Aruzhan Yessilbekova, Olzhas Konakbayev Rashitdin Kokenov

Proactive Cyber Threat Intelligence and Detection in Penetration Testing Using Machine Learning Techniques 954
Saule T. Amanzholova, Ademi Tursynkozha, Dauren Minkebay, Kundyz Zhumazhanova, Aigerim Alibek

CAIP-Pentest: A Causal and Interpretable Agent Framework for Autonomous Web Vulnerability Exploration 961
Nadia Ait Oufqir, Meriem Mandar, Anas Rachid

A Hybrid Software Protection Framework Against Reverse Engineering Using AST Obfuscation and Runtime Code Encryption 967
Askaruly Abinur, Saule T. Amanzholova, Shangytbayeva Gulmira, Yelepbergenova Aigul Zhussupbayeva Marzhan, Shamisheva Bibigul

Development of a Private LTE/5G Experimental Platform for Attack Simulation and Security Hardening with Open-Source Solutions 973
Alisher Yeslyambek, Demid Katkov, Akhmet Tussupov, Almat Buralkiyev, Gulzhan Kashaganova

Models and algorithms for protecting intrusion detection systems from attacks on machine learning components 980
Murat Akhmetov, Nursultan Momyn, Alikhan Mukhametkan, Nurzhas Bolatbekov

AI-Enabled Voice Cloning and Spoofing Risks in Speaker Verification Systems: A Comparative Analysis of Empirical Evidence 985
Cesar A. Nuñez, Dariga Zhaksylyk, Merey Altaikyzy, Adlet Kalimullin, Aleksander Lebedev Svetlana Dusenko

Agentic AI Security in IoMT: A PRISMA-Guided Scoping Review and Layered Threat–Defense Taxonomy 991
Batyrkhan Abylkan, Darkan Serik, Askhar Mussa, Syrym Sapash, Aibolat Kurakbayev, Saule Amanzholova

Multi-Class Hazardous Content Recognition in Forensic Imagery: A Hybrid Labeling and Vision Transformer Approach 997
Perizat Tazhibayeva, Yonghao Wang, Aigerim Alibek, Assel Khassanova

Attacks via AI Agents: How Autonomous Systems Are Becoming the New Weapon of Cybercriminals 1003
Daniyar Segizbayev, Karabalin Bakhtiyar, Orynbasar Sultan, Shuktaev Abzal

Prompt Injection as the New SQL Injection: The Emergence of Attacks on AI Reasoning 1009
Shuktaev Abzal, Karabalin Bakhtiyar, Orynbasar Sultan, Olga Orlova, Elena Aleksandrovna Korochkina Sholpan Borashova

Deepfake Technologies as a Cybersecurity Threat in Digital Environments 1015
Shambulov Ulykbek, Dair Uzakov, Nurlan Orynbassar, Ilhami Colak, Kairolla Nurali, Korhan Kayisli

Zero Trust Architecture 1021
Aidar Ispussinov, Ilyas Sailaubekov, Nurzhan Syzdyk, Bekarys Nurzhaubaev, Bakdaulet Argyngazy Nurzhan Syzdyk

Behavioral Biometrics for Continuous Authentication in Cybersecurity Systems 1026
Aidar Ispussinov, Ilyas Sailaubekov, Nurzhan Syzdyk, Bekarys Nurzhaubaev, Bakdaulet Argyngazy Nurzhan Syzdyk

Cloud Misconfiguration as a Leading Cause of Data Breaches: Analysis and Prevention Strategies 1031
Dinara Chsheglova, Karim Almukhanov, Dinmukhammed Balabek, Beksultan Tulepbergen Olzhas Konakbayev

Detection of Malicious Files in Network Traffic Using Machine Learning 1036
Maksat Meshituly, Zhaksybek Dias, Alisher Batkuldin, Rakhman Khamzanov, Medina Nurbek Aldiyar Zholynbet

Development of a Method of protection against cyber attacks on the payment system 1040
Khikmetov Askar, Amina Adilkhan, Venera Boltan, Zhanel Tolesh

Deepfakes and identity theft in the age of AI 1047
Assel Nurguzhina, Zukhra Sarsenbi, Saltanat Umbetalina, Aldiyar Kaldybek

Development of an Automatic Notification System for Unauthorized Activities on the Local Network 1053
Murat Akhmetov, Yerassyl Omarzhanov, Yerassyl Aikenov, Arsen Shegebay

Security Challenges and Countermeasures in Next-Generation Networking: A Comprehensive Survey of 5G, 6G, SDN, and NFV Vulnerabilities 1058
Isakhan Birzhan, Sherbadalova Zumrad Odiljonovna, Nurlanova Asem Nurlanovna

The Impact of Agent-Inspired Rule Layers on ML Intrusion Detection 1064
Maksat Meshituly, Zhibek Mussakulova, Didar Kairanbayeva

1) HybridPhish: A Weighted Ensemble Approach for High-Precision Phishing URL Detection Using Lexical and Host-Based Features 1070
Bayekeshova Bilimgul, Aman Nurkhan, Abdizhali Aset

AI as a tool for cyber attacks 1076
Shuteyeva Gulnur, Zukhra Sarsenbi, Saltanat Umbetalina, Aldiyar Kaldybek

CAL-CTI: A Continual Adversarial Learning Framework for LLM-Based Cyber Threat Intelligence Under Non-Stationary Distributions 1081
Meryem Lirsi, Meriem Mandar, Yassine Bnslimane

Behavioral Risk Scoring for Predicting User Vulnerability to Social Engineering Attacks: A Random Forest and Isolation Forest Hybrid Approach 1086
Dias Berlibek, Aigul Shaikhanova, Arailym Medetbek

Private Browsing Under the Microscope: Residual Artifacts in Firefox 1091
Arsen Shegebay, Soltanbay Kunnur, Borashova Sholpan, Aliya Zhetpisbayeva

HERO-WM: A Hybrid Evidence-Recoverable Watermarking Framework for Image Integrity Verification under Platform Transformations 1096
Merei Zhaparkhanova, Alissa Ryzhova, Natalya Glazyrina, Gerald Feldman, Alibek Bektaev, Meiir Raikhan

Comparative Reliability of Chip-Off and Logical Methods in SSD Forensic Analysis 1102
Leila Rzayeva, Aliya Zhetpisbayeva, Aigerim Alibek, Perizat Tazhibayeva

Multimodal Enterprise Authentication Resistant to AI-Based Identity Manipulation: Facial Anti-Spoofing and Multilingual Deepfake Speech Detection 1107
Usmanov Mansur, Leila Rzayeva, Rayymbekov Miras, Aigerim Alibek

LIME vs. SHAP: A Quantitative Comparison of Local Explanation Methods for Random Forest Classifiers 1113
Kaliyeva Samal, Sadykbek Miras, Kairat Sultan

LeafSense: CNN-Based Plant Disease Detection System for Smart Agriculture 1119
Ece Yuksektepe, Esra Ozdemir, Guray Yilmaz

Integration of Blockchain Technology into a Correspondence Analysis Service for Ensuring Digital Evidence Integrity in Forensics 1125
Leila Rzayeva, Daniil Pogolovkin, Starovoitova Yana, Aliya Ospanova, Zhankulov Daniyar Kurmangali Yelzhas

Automated Security Assessment and Risk Scoring for IoT Devices via Network Scanning 1130
Sena Bilgin, Cem Günal, Özgür Koray Şahingöz

ADR-Fusion: A Multi-modal Deep Learning Framework for Dynamic Drug Safety and Explainable Clinical Decision Support 1136
Miray Sude Mutlu, Beril Gungor, Ozgur Koray Sahingoz

Mommyira: A Machine Learning Framework for Postpartum Depression Risk Prediction 1143
Dilara Yılmaz, Miraç Müberra Gül, İkra Sarıçiçek

LLM-Orchestrated Multi-Agent Framework for Android Malware Detection from APK Analysis 1151
Halime Sila Ozyurt, Selma Akkok, Ozgur Koray Sahingoz

MinervAI: Multi-LLM Powered Autonomous Cyber Threat Intelligence for Ransomware Analysis 1159
Miraç Müberra Gül, İkra Sarıçiçek, Dilara Yılmaz

TriShield: Toward an Autonomous and Self-Evolving Cyber Defense via Predictive SOC, Causal Pentest Agents, and Adversarial LLM-CTI 1167
Meryem Lirsi, Fatima Benettaj, Nadia Ait Oufqir, Meriem Mandar

Automated Personnel Trustworthiness Assessment as a Cybersecurity Control: Mitigating Ideologically-Motivated Insider Threats in Critical Financial Infrastructure 1172
Zamir Khailudayev

Deepfake Technology and Cybercrime: Identity Manipulation in the AI Era 1179
Shambulov Ulykbek, Armanuly Abilmansur, Mynzhassarov Ilyas, Kalikhan Nursultan

Zero-Trust Architecture with Continuous AI-Based Risk Scoring for Dynamic Access Control 1183
Nurkhat Ibadildin, Alisher Batkuldin, Nurzhan Bekmurat, Shavkat Khanezar

Hybrid Static-Dynamic Malware Detection Using Lightweight Feature Fusion 1189
Kazybek Nurzhigit, Alisher Batkuldin, Nurzhan Bekmurat, Shavkat Khanezar

Predicting User Susceptibility to Phishing Attacks Using Behavioral Feature Engineering for Adaptive Cybersecurity Training 1194
Yedige Radolda, Dina Satybaldina, Aigul Shaikhanova, Raikhan Muratkhan

Zero-Shot Prompt Injection Detection via N-gram Pooling of Token-Level Hidden States 1198
Lokesh Prakash Manohar

Etiology-Aware Radiopathomic Fusion for Hepatocellular Carcinoma Recurrence Prediction: Disentangling HBV, NASH, and Alcohol-Driven Signatures from Paired CT and Whole-Slide Histology 1204
Gunjan Vasant Ramteke

Etiology-Stratified Spatial Immune Topology Learning in Hepatocellular Carcinoma via Hierarchical Graph Attention Networks on 37-Plex CODEX Proteomics 1211
Gunjan Vasant Ramteke

Cross Domain NeuroFusion Attention with Gradient Guided Multi Scale Deformable Spatial Attention Network for Brain Tumor Detection in CT and MRI 1217
Binu John J N, L. Nisha Evangelin

Detecting AI-Generated Phishing Campaigns Using Linguistic Forensics and Machine Learning 1222
Azamat Auyezov, Arslan Abdigali, Yerkuat Dota, Kairat Zhunussov, Bekarys Nurzhaubaev

Identity and Access Management for Agentic AI: A Zero-Trust Security Framework 1228
Altynbek Makhmetov, Yerkuat Dota, Azamat Auyezov, Arslan Abdigali, Kairat Zhunussov

Empirical Evaluation and Optimization of Multi-RAT Digital Indoor Systems in Healthcare Environments: A 3G/4G/5G LampSite Deployment 1233
Asma Ali Budalal, Omnia Saleh Elshlmany

Evaluating Artificial Intelligence for Predicting and Interpreting Molecular Toxicity from Chemical Structures to Enhance Early Drug Screening 1239
Daniel Ndifreke Samuel, Ogunlola John Olalere, Celestine Iwendi, Adedeji Edward Adesola Afeez Oluwaseun Akande, Blessing Alice Alao-Olatunji

AI Supply Chain Attacks: Risks in Pretrained Models and Third-Party Integrations 1245
Armanuly Abilmansur, Mynzhassarov Ilyas, Kalikhan Nursultan

Cyber-Physical PWM Duty Cycle Manipulation Attacks on DC-DC Boost Converters 1249
Sahin Coskun, Erdal Bekiroglu, Erdal Irmak

A Hybrid DenseNet–Vision Transformer Framework for Diabetic Retinopathy Classification 1255
Mysha Samiha Priota, SK Fahema Mahajabin, Maharun Fahamida Maysha, Fazley Rabbi Md. Imran Hossen, Md. Shifatul Ahsan Apurba, Md. Arman Hosen Patoary, Md. Yasin Arafat Tamim Tauhidur Rahman Sakib

From AI Strategy to Executable Controls: A PRISMA-Guided Systematic Review of AI Governance for Cybersecurity Efficiency in Azerbaijan 1261
Leyla Tarlan Dadashova, Rahid Zahid Alekberli

An integrated optimization of a stand-alone DC nanogrid-based battery swapping station 1268
İzviye Fatımanur Tepe, Oğuz Taşdemir, Erdal Irmak

Inference-Time AI Safety in Edge-Deployed Autonomous Systems: A Multi-Run Empirical Evaluation of the Kerimov-Alekberli Information-Geometric Framework 1275
Rahid Zahid Alekberli, Hikmat Karimov

StickyMemory: Robust Web Agents with Episodic Memory and Self-Verification 1281
Nithesh Gudipuri

A Multi-Paradigm AI Framework for Real-Time Anomaly Detection and Adaptive Risk Scoring in Digital Payment Ecosystems 1287
Kushal Bhatt

Features of intelligent cryptographic protection for IoT devices 1293
Atanov S.K., Seitkulov Y.N., Auyezov A.S.