cirf.co.in

CIRF
Excellence in Innovation

Abstract Proceedings of the CIRF International Virtual Conference on

AI, Data Science & Cybersecurity (CIRF-IVC-ADSC 2026)

March 2026

Organized by:

Computational Intelligence Research Foundation (CIRF)

India

ISBN: 978-81-999525-0-8

CIRF International Virtual Conference on AI, Data Science & Cybersecurity (CIRF-IVC-ADSC 2026)

Date: March 28, 2026

Organized by,

Computational Intelligence Research Foundation

Conference Chairs

Dr D Doreen Robin M.E., Ph.D.,
Founder & Director

Director,
Computational Intelligence
Research Foundation, India

Dr C R Rene Robin M.E., Ph.D
Director, CIRF

Dean – Innovation,
Sri Sai Ram Engineering
College, India

ISBN: 978-81-999525-0-8

Published by:
Computational Intelligence Research Foundation (CIRF)
India

CIRF International Virtual Conference on AI, Data Science & Cybersecurity (CIRF-IVC-ADSC 2026)

Date: March 28, 2026

Preface

The CIRF International Virtual Conference on AI, Data Science & Cybersecurity (CIRF-IVC-ADSC 2026) brings together researchers, academicians, and industry experts to discuss emerging trends and innovations.

This abstract proceedings volume presents selected research contributions accepted for presentation at the conference.

This publication is officially released with ISBN: 978-81-999525-0-8.

CIRF International Virtual Conference on AI, Data Science & Cybersecurity (CIRF-IVC-ADSC 2026)

Date: March 28, 2026

KEYNOTE SPEAKER

Dr. Kabaly P. Subramanian PhD

Former Dean, Faculty of Business Studies

Arab Open University, Oman

SESSION CHAIR TRACK -1 | 10:15 AM – 12:30 PM

Dr. Golda Dilip Professor & HOD

Department Of Computer Science And Engineering

SRM IST Vadapalani Campus

SESSION CHAIR TRACK -2 | 1:15 PM – 3:30 PM

Dr. G. Adiline Macriga B.E., M.E., Ph.D

Professor/ IT Sri Sai Ram Engineering College, Chennai

CIRF International Virtual Conference on AI, Data Science & Cybersecurity (CIRF-IVC-ADSC 2026)

Date: March 28, 2026

The Organizing Committee extends sincere gratitude to the Advisory Committee members for their guidance and support.

Conference Advisory Committee

S.No	Name	Affiliation	Country
1	Mohammadhosein Ahmadi	Shahrood University of Technology	Iran
2	Kabaly P. Subramanian	Arab Open University	Oman
3	Padmaja P	Oracle	United States
4	Radhika Pandiyan	Global Knowledge Technologies	India
5	Easwarakumar K S	Professor	India
6	Dafni Rose	St. Joseph's Institute of Technology	India
7	Belina V. J. Sara	SRM Institute of Science and Technology	India
8	Esther Hannah	Women's Christian College	India

CIRF International Virtual Conference on AI, Data Science & Cybersecurity (CIRF-IVC-ADSC 2026)

Date: March 28, 2026

We acknowledge the valuable contributions of the Technical Review Committee for ensuring the quality and integrity of the selected abstracts.

Technical Program Committee

S.No	Name	Affiliation	Country
1	Amit Prasad	Tata Consultancy Services	United States
2	Anand K Singh	AbbVie Inc.	United States
3	Bhavya Mehta	Fortinet	United States
4	Chaitanya Bharath Somineni	Toyota Motor Credit Corporation	United States
5	Chetan Prakash Ratnawat	Capgemini America Inc.	United States
6	Dafni J Rose	St. Joseph's Institute of Technology	India
7	Devkiran Narayana	USAA	United States
8	Dr N. Jayashri	Dr. M.G.R Educational and Research Institute	India
9	Felicia J Lilian	Thiagarajar College of Engineering	India
10	Hardeep Singh Tiwana	Amazon Web Services	United States
11	Harikrishnan Ramakrishna Pillai	Walmart Inc	United States
12	Harvendra Singh	Publix Super Markets Inc	United States
13	Janarthanan P	Sri Venkateswara College of Engineering	India
14	Kalaiselvi K	Saveetha Institute of Medical and Technical Sciences	India
15	Karteek Sonapuram	GEICO	United States
16	Krishna Suman Dara	HPE	United States
17	Lahari Popuri	USAA	United States
18	Lavanya Anandham	Auxilium College	India
19	Maulik Bhatt	Amazon	United States

Technical Program Committee

S.No	Name	Affiliation	Country
21	Niranjan Yadavali	Salesforce (Tableau)	United States
22	Nirmal Jingar	Wayfair	United States
23	Padmaja Pulivarthy	Samsung	United States
24	Ponsankar Semmandampalayam	Walmart Inc	United States
25	Preethi S R	SRM Valliammai Engineering College	India
26	Premalatha J Prabhakaran	Dhanalakshmi Srinivasan University	India
27	R. Kannamma	Prathyusha Engineering College	India
28	Rachel Nallathamby	Vel Tech	India
29	Rajendran Renganathan	Capital One	United States
30	Rajesh Mannam	Gilead Sciences	United States
31	Ramya Vani Rayala	University of the Cumberlands	United States
32	Ravi Teja Medempudi	Fidelity Investments	United States
33	Ravi Teja Pagidoju	Independent	United States
34	Sakshi Gupta	Harvey AI	United States
35	Sanatya Singh	Munich Reinsurance	Germany
36	Sanjay Poddar	Fortinet	United States
37	Shatrughna Upadhyay	Intuit Inc	United States
38	Shilpi Yadav	IBM	United States
39	Sibaram Prasad Panda	Decision Ready Solutions	United States
40	Sivamurugan Perumal	Nous Infosystems	United States

Technical Program Committee

S.No	Name	Affiliation	Country
41	Tirumala Kishore Palem	Lumen IT Services	United States
42	Veera Venkata Uday Kumar J	American Express Global Business Travel	United States
43	Vivek Katarya	LinkedIn Inc	United States
44	Amit Mendiratta	Microsoft	United States
45	Jasmine Gabriel	Rajalakshmi Engineering College	India
46	Jasmine R L	College of Engineering, Guindy	India
47	Ashwin Conjeevaram Sundaravadanam	Apple	United States
48	David Raj G	B S Abdur Rahman Crescent Institute	India
49	Divija Ganiga	Personal	United States
50	Dr Golda Dilip	SRM Institute of Science and Technology	India
51	Esther Hannah M Moses	Women's Christian College	India
52	Naveen Kumar Reddy Paiiuri	Amazon	United States
53	Shiny Duela	SRM Institute of Science and Technology	India
54	Vanitha N	Sri Sairam Institute of Technology	India
55	Vivek Madan	Fortinet Inc	United States
56	Anup Kagalkar	Independent Researcher	India
57	Bhushan B Chaudhari	Iris Software	United States
58	Rajesh Remala	Independent Researcher	India
59	Satish Kabade	Independent Researcher	India
60	Akshay Sharma	Independent Researcher	India

Table Of **Content**

About **Company**

CIRF is a Section 8 Company, registered under the Ministry of Corporate Affairs, Government of India.We are a certified organization with 12A and NGO Darpan certifications.
At CIRF, we empower individuals and institutions through nature-inspired algorithms and cutting-edge technologies.
We collaborate with leading academic and industrial partners to foster innovation and drive impactful research in the field of computational intelligence.

The Computational Intelligence Research Foundation (CIRF) is dedicated to promoting research, innovation, and knowledge exchange in emerging areas of computational intelligence and digital technologies. The foundation brings together academicians, researchers, industry professionals, and students to create a collaborative environment that encourages interdisciplinary learning and technological advancement. By facilitating academic partnerships and research collaborations, CIRF supports the development of innovative solutions that address real-world challenges and contribute to the advancement of science and technology.

Through its initiatives, CIRF organizes conferences, workshops, training programs, and innovation bootcamps that enable researchers and students to share ideas and present their work. The foundation also supports skill development and research mentoring while promoting a strong culture of innovation and knowledge sharing.

CIRF-IVC-ADSC 2026 | ISBN: 978-81-999525-0-8

About the Conference

The CIRF International Virtual Conference on AI, Data Science & Cybersecurity (CIRF-IVC-ADSC 2026) marks the first edition of this prestigious global initiative, conducted in a virtual mode on March 28, 2026, enabling broad national and international participation.

With the theme "Empowering Innovation through AI, Data Science & Cybersecurity", the conference was conceived as a dynamic platform to bring together researchers, academicians, industry professionals, and students to exchange knowledge and explore emerging trends in these rapidly evolving domains.

The conference witnessed an overwhelming response from the research community, receiving a total of 194 paper submissions from authors across India and the United States. Each submission underwent a rigorous and structured peer-review process conducted by a dedicated panel of 60 expert reviewers, ensuring high standards of quality, originality, and relevance.

Following this comprehensive evaluation, 21 papers were selected for acceptance, resulting in a competitive acceptance rate of approximately 10.8%, reflecting the quality and selectivity of the conference. These accepted works represent impactful and innovative research contributions addressing real-world challenges in intelligent systems and digital security.

Selected high-quality papers presented at the conference will be recommended for publication in reputed journals of Imanager Publications. All shortlisted papers will undergo an additional round of peer review as per the journal's editorial policies. Upon successful completion of the review process and meeting the required standards, the papers will be considered for publication. The journals are indexed in Google Scholar, ensuring wider visibility and accessibility of the published research to the global academic community.

As the inaugural edition, CIRF-IVC-ADSC 2026 establishes a strong foundation for future conferences, fostering collaboration, interdisciplinary learning, and continued research excellence in critical technological domains.

CIRF-IVC-ADSC 2026 | ISBN: 978-81-999525-0-8

CIRF
Excellence in Innovation

Director **Message**

It gives me immense pleasure to present the Abstract Proceedings of the CIRF International Virtual Conference on AI, Data Science & Cybersecurity (CIRF-IVC-ADSC 2026), published with ISBN: 978-81-999525-0-8.

Dr D Doreen Robin M.E., Ph.D.,
Founder & Director

In today's rapidly evolving digital era, the convergence of Artificial Intelligence, Data Science, and Cybersecurity is shaping the future of innovation, research, and societal transformation. This conference has been envisioned as a dynamic platform to bring together academicians, researchers, industry experts, and students to share knowledge, exchange ideas, and explore emerging trends in these critical domains.

The abstracts compiled in this volume reflect the intellectual rigor, creativity, and research excellence of the contributors. Each submission has undergone a structured review process to ensure quality and relevance, addressing contemporary challenges and future opportunities in technology and security.

I extend my sincere gratitude to the keynote speaker, session chairs, advisory members, and technical review committee for their invaluable contributions and guidance. My appreciation also goes to all the authors and participants whose enthusiasm and commitment have made this conference a meaningful academic endeavor.

I am confident that this proceedings volume will serve as a valuable resource for researchers, practitioners, and students, inspiring further exploration and innovation in the fields of AI, Data Science, and Cybersecurity.

Wishing the conference great success and impactful outcomes.

Dr. D. Doreen Robin
Director
Computational Intelligence Research Foundation (CIRF)

Director
Message

It is with great pride and pleasure that I extend my greetings to all participants, contributors, and organizers of the CIRF International Virtual Conference on AI, Data Science & Cybersecurity (CIRF-IVC-ADSC 2026).

Dr C R Rene Robin M.E., Ph.D.,
Director - CIRF
Dean Innovation & Professor CSE
Sri Sairam Engineering College

In an age where technology is rapidly transforming every aspect of our lives, the integration of Artificial Intelligence, Data Science, and Cybersecurity has become not only relevant but essential. This conference serves as a significant platform for fostering innovation, encouraging interdisciplinary collaboration, and addressing real-world challenges through cutting-edge research.

The Abstract Proceedings, published with ISBN: 978-81-999525-0-8, represent a collection of insightful contributions from researchers and practitioners across diverse domains. The quality of the submissions reflects the dedication, creativity, and scholarly commitment of the authors, as well as the rigorous efforts of the review committee.

I would like to express my sincere appreciation to the keynote speaker, session chairs, advisory members, and technical reviewers for their invaluable support in ensuring the success of this conference. I also commend the organizing team for their meticulous planning and execution.

I am confident that this conference will not only facilitate meaningful knowledge exchange but also inspire future research and collaborations in the fields of AI, Data Science, and Cybersecurity.

Wishing the conference every success and continued impact in advancing technological excellence.

Dr. C. R. Rene Robin, Ph.D.
Director
Computational Intelligence Research Foundation (CIRF)
Dean Innovation & Professor CSE ,Sri Sairam Engineering College

CIRF
Excellence in Innovation

Vision & Mission

Vision

To contribute nation building through mentoring and innovation.

Mission

- Undertake product development activities in emerging thrust areas.
- Support higher education institutions to establish Innovation Ecosystem
- Introduce courses based on the Industry & Societal demands
- Collaborate with Institutions, research and development organizations and Industries.
- Serve the community at large.

CIRF-IVC-ADSC 2026 | ISBN: 978-81-999525-0-8

CIRF
Excellence in Innovation

CIRF-IVC-ADSC 2026 - Track 1

AI, Data Science & Intelligent Applications

CIRF-IVC-ADSC 2026 | ISBN: 978-81-999525-0-8

CIRF International Virtual Conference on AI, Data Science & Cybersecurity | 2026

cirf.co.in

LegalBot: A RAG-based Multilingual Chatbot for Legal Assistance

Padidala Bharath Chandra Rao , Bokka Ashish Reddy, B. Ramadasu
Computer Science and Engineering, Chaitanya Bharathi Institute of Technology
Hyderabad, Telangana, India
bharathrao0015@gmail.com, ashishreddy1746729@gmail.com, bramadasuu cse@cbit.ac.in

Abstract—
Understanding complex legal documents, such as national constitutions, is challenging due to their technical language and structure. Conventional search techniques often fail to capture the semantic meaning of user queries, while linguistic diversity in India further limits access to legal information, which is predominantly available in English. Although Large Language Models (LLMs) can generate human-like responses, they may produce outdated or inaccurate information, commonly referred to as hallucinations, which is particularly critical in the legal domain.
Retrieval-Augmented Generation (RAG) enhances LLMs by retrieving relevant information from trusted sources and using it to generate accurate responses. This paper explores the application of RAG in AI-based legal assistants, addressing challenges such as document chunking and efficient information retrieval. The proposed system, LegalBot, is designed to provide clear and concise responses about the Indian Constitution in multiple languages.
LegalBot stores constitutional data in a ChromaDB vector database, uses the all-mpnet-base-v2 model for semantic understanding, and generates responses through the Ollama Mistral LLM, supported by translation and simplification mechanisms. Experimental results show that LegalBot effectively retrieves relevant constitutional information and delivers precise, understandable responses, demonstrating the potential of RAG in improving access to legal knowledge in India.
Keywords— Retrieval-Augmented Generation (RAG), Large Language Models (LLM), Legal Technology, Legal AI, Chatbot, Indian Constitution, Ollama, ChromaDB, Vector Database, Natural Language Processing (NLP), Access to Justice, Multilingual, Legal Simplification.

ONLINE PAYMENT FRAUD DETECTION USING MACHINE LEARNING

Ms. S. Aiswarya Priyadarshini - Assistant professor**, Manoj V, Pragatheeswaran M, Sakthivel B**
Computer Science and Engineering(Cyber security) , Sri Sairam Institute of Technology, Chennai
aiswaryapriyadarshini.sc@sairamit.edu.in, sit22sc031@sairamtap.edu.in, sit22sc013@sairamtap.edu.in, sitl23sc03@sairamtap.edu.in

Abstract – In this digital age, online payment systems have become integral to personal and business transactions, making them prime targets for cybercriminals. This project aims to develop a comprehensive solution to detect phishing links and prevent fraudulent transactions, with a particular focus on phishing attacks facilitated through malicious links, so we Utilizing advanced machine learning algorithms to detect phishing link, regarding this, we include one extension into the browser once witch ON the extension, which will automatically analyze URLs shared across social media platforms, such as WhatsApp and Telegram, Instagram, etc to determine their reliability and origin of the link. Upon detecting a potentially fraudulent or phishing link, users will be blocked from proceeding to the site and redirected to a warning using this extension to secure the user.

CIRF-IVC-ADSC 2026 | ISBN: 978-81-999525-0-8

MALWARE DETECTION USING MACHINE LEARNING

Ms. Aiswarya Priyadarshini S - Assistant Professor, Dhineshwaran M, Aathiganesh S, Charan Deepak M - UG Scholar,
Dept of Computer Science and (Cyber Security), Sri Sai Ram Institute of Technology,
aiswaryapriyadarshini.sc@sairamit.edu.in, sit22sc028@sairamtap.edu.in,
sit22sc038@sairamtap.edu.in, sit22sc005@sairamtap.edu.in

Abstract—

Malware continues to pose a significant threat to modern computing systems due to its rapidly evolving nature and increasing sophistication. Traditional detection methods, such as signature-based antivirus systems, struggle to identify new and unknown malware variants, particularly zero-day and polymorphic threats. This paper presents a machine learning-based malware detection framework designed to classify executable files as either benign or malicious using behavioral and metadata-based features.

A dataset of 10,000 executable samples, including 6,000 malicious and 4,000 benign files, was collected and used to train and evaluate Decision Tree, Random Forest, and Neural Network models. The dataset was split into training, validation, and testing sets to ensure reliable evaluation.

Experimental results show that the Decision Tree classifier achieved an accuracy of 88.5%, Random Forest achieved 95.6%, and the Neural Network model performed best with 96.4% accuracy, along with high precision, recall, and F1-score. These findings highlight the effectiveness of machine learning techniques in improving malware detection compared to traditional approaches.

Keywords— Malware Detection, Cybersecurity, Machine Learning, Decision Trees, Neural Networks, Real-Time Monitoring.

Real-Time Detection and Health Classification

Dr.B.Arunsundar - Associate Professor**, Hasini Repaka, Syam Kumar O, Ch.S.K.Gowtham -** UG Student
Department of of Data Science and Business Systems, School of Computing, College of Engineering and Technology,SRM Institute of Science and Technology, Kattankulathur, Chennai, India
knr6785@srmist.edu.in, so3230@srmist.edu.in, sc2927@srmist.edu.in, arunsunb@srmist.edu.in

Abstract - This research introduces a cutting-edge framework leveraging advanced AI and IoT technologies to revolutionize lion conservation. The primary focus is on real- time lion detection, individual identification using unique facial features, gender classification, and health condition assessment, including malnutrition, injuries, and illnesses. By integrating GPS modules and IoT sensors, the system facilitates non- invasive and ethical monitoring of lions and their habitats. The study employs YOLO (You Only Look Once) for real-time detection of lions in video feeds and EfficientNet B7 for multi- task classification, enabling precise identification of individual lions and their health status. DeepSORT is utilized for tracking lion movements over time, ensuring continuous observation and territorial mapping. These models are deployed on edge devices, such as drones and camera traps, to deliver instantaneous results while minimizing latency. The proposed system offers numerous advantages, including improved conservation efforts through real-time alerts and actionable insights. Its ability to monitor health conditions and movement patterns enables proactive interventions to safeguard lion populations. Moreover, the integration of IoT sensors ensures comprehensive environmental monitoring, supporting a holistic understanding of the ecosystem. By employing cloud platforms for data analytics and storage, the system provides accessible dashboards and detailed reports, empowering conservationists and wildlife authorities with valuable insights. This framework not only enhances the efficiency of lion conservation but also ensures ethical practices, setting a benchmark for integrating AI and IoT in wildlife preservation. The research underscores the potential of technology to address critical ecological challenges and promote sustainable conservation efforts.

keywords - Lion Monitoring, Wildlife Conservation, Drones, DeepSORT, Animal tracking , EfficientNet B7, Deep Learning.

Voxel-Reduced SegFormer3D: Efficient 3D Brain Tumor Segmentation via Wavelet-Enabled Spatial Compression Under Limited GPU Resources

Karthik Teja, Ramavath Babu Singh, Dharavath Indu, Dr. A Naresh Kumar
Department of Computer Science and Engineering, Institute of Aeronautical Engineering College, Dundigal, Hyderabad, India
22951A6753@iare.ac.in, 22951A6715@iare.ac.in, 23955A6707@iare.ac.in, a.nareshkumar@iare.ac.in

Abstract - High-resolution 3D brain tumor segmentation using multimodal MRI suffers from severe limitations because of the "voxel explosion" problem. This problem occurs when a 240×240×155 MRI volume contains approximately 8.9 million voxels, which results in excessive token counts and quadratic attention complexity in transformer-based models. This renders training infeasible on limited hardware such as dual NVIDIA T4 GPUs (~30 GB VRAM). We propose Voxel-Reduced Seg-Former3D (VR-SegFormer3D), which applies 3D Haar wavelet decomposition at the input stage to retain only the low-frequency (LLL) sub-band, achieving an 8× voxel reduction (to ~1.1 million voxels) while preserving essential global anatomical structures for hierarchical transformer encoders. The compressed volumes feed a memory-efficient Mix Transformer (MiT) encoder with spatial reduction attention and a lightweight MLP decoder, further optimized via mixed precision training and gradient checkpointing. On the BraTS 2020 dataset, VR-SegFormer3D achieves a mean test Dice score of 0.722 ± 0.130 and IoU of 0.579 ± 0.138 across 33 cases, outperforming the baseline SegFormer3D (Dice 0.68) and constrained nnU-Net (Dice 0.72) under identical 30 GB constraints. These results demonstrate that early-stage voxel reduction is a powerful strategy for enabling high-fidelity 3D transformer-based segmentation in resource-limited environments.

keywords - Brain tumor segmentation, 3D MRI, Trans-former, Wavelet decomposition, Voxel reduction, SegFormer, BraTS 2020, Memory-efficient deep learning

ClimaVision: Deep Learning for Short-Term Atmospheric Forecasting

Dr. Elumalaivasan P - Associate Professor**, Vutukuru Sathya Sai Harshit, Harshita Handa, S. Sai Charani -** UG Student
Department of Data Science and Business Systems School of Computing
SRM Institute of Science and Technology (SRMIST)
Kattankulathur, India
elumalap3@srmist.edu.in, sv0671@srmist.edu.in, hh5758@srmist.edu.in, ss2655@srmist.edu.in

Abstract – Accurate short-term atmospheric forecasting is essential for climate monitoring, disaster management, and environmental planning. Traditional numerical weather prediction models require significant computational resources and may struggle to capture complex nonlinear atmospheric patterns. This study presents ClimaVision, a deep learning-based framework for short-term atmospheric prediction using ERA5 reanalysis data. The proposed system leverages historical atmospheric variables including temperature, sea level pressure, wind components, and
cloud cover to forecast future atmospheric conditions. Multiple deep learning models, including Long Short-Term Memory (LSTM), Graph Neural Networks (GNN), Transformer, and NBEATS, are implemented to capture spatiotemporal dependencies in atmospheric data. The models are trained using historical sequences of atmospheric observations and evaluated using standard regression metrics such as Mean Squared Error (MSE), Mean Absolute Error (MAE), and R^2 score. Experimental results demonstrate that deep learning models can effectively learn atmospheric patterns and provide reliable short-term forecasts. The proposed ClimaVision framework highlights the potential of AI-driven approaches for improving atmospheric prediction
systems.

keywords – Atmospheric forecasting, Deep learning, ERA5 dataset, Time-series prediction, LSTM, Transformer, Graph Neural Networks.

Text Summarization Using Deep Learning Transformers

Dr. G Ganapathi Rao, Bhanu Tej P, B Harsha vardhan yadav, M Harshitha
Department Of CSE(Data Science), Institute of Aeronautical Engineering, Dundigal, Hyderabad, India.
g.ganapathirao@iare.ac.in, paillabhanutej5@gmail.com, harshavardhanyadav24@gmail.com, harshitha12345@gmail.com

Abstract – The increase in the number of digital texts in various fields including news articles and scientific papers has resulted in the need for text summarization systems. The Transformer model has helped in improving the results for text summarization systems through its recent inclusion in the systems. The model requires a lot of computational resources for its functioning. The authors have proposed a lightweight model for text summarization based on the concept of a hybrid fusion approach. The
extractive part of the model helps in identifying the important sentences in the text through the BERT-Tiny model along with weak supervision using the ROUGE model. The abstractive part of the model is based on the DistilBART model as the main concept for the model since the model generates text through its sequence-to sequence method. The results obtained from the models are then fed into the T5-Small model for generating the summary based on the important information in the two summaries. The proposed framework is evaluated on a multi-domain hybrid dataset consisting of news articles, scientific papers, legal documents, and conversational dialogues. Experimental results demonstrate that the proposed fusion pipeline maintains low computational complexity while achieving ROUGE-1, ROUGE-2, and ROUGE-L scores of 0.4045, 0.2167, and 0.3197 respectively on the test dataset.

keywords – Text Summarization, Hybrid Summarization, Extractive Summarization, Abstractive Summarization, Transformer Models, ROUGE Metrics

Ancient Tamil Inscription Recognition and Semantic Reconstruction using Deep Learning and Vision Language Models

Dr. K. Dhanasekaran, Pachaiyappan M
Department of Data Science and Business Systems
Department of Computational Intelligence
SRM Institute of Science & Technology, Kattankulathur
Chennai, Tamil Nadu, India
dhanasek1@srmist.edu.in, pm5186@srmist.edu.in

Abstract - Ancient Tamil inscriptions are valuable sources of historical information; however, interpreting them is both complex and time-consuming. This paper proposes a web-based system for the recognition and analysis of ancient Tamil inscription characters using deep learning techniques.
Character recognition is performed by training a Convolutional Neural Network (CNN) on a dataset of 1,697 inscription images spanning 27 character classes. The system supports both single-character recognition and multi-character sequence processing. For sequences of characters, the identified outputs are further processed to construct meaningful Tamil words and provide corresponding textual explanations.
The proposed model achieves an accuracy of 97.94%, demonstrating its effectiveness in handling the complex patterns found in ancient inscriptions. The system features a user-friendly interface that includes secure access, image upload, visualization, chatbot interaction, and prediction history tracking.
Furthermore, the system leverages the Gemini Vision-Language Model (VLM) to integrate visual inputs with textual prompts, enabling accurate interpretation, contextual understanding, and semantic extraction from Tamil inscription images. By combining CNN-based visual recognition with automated textual analysis in a web-based environment, the proposed solution contributes significantly to the study and preservation of ancient Tamil heritage.

Keywords - ancient tamil inscriptions, convolutional neural network (cnn), character recognition, deep learning, ai-based word analysis, cultural heritage preservation

Named Entity Recognition Using Deep Transformers

Kornu Kavya, Bandi Jeevani, Kuriyan Meghana, Dr. A Naresh Kumar
Department Of CSE(Data Science), Institute of Aeronautical Engineering, Dundigal, Hyderabad, India.
Kavyakornu2004@gmail.com, jeevanibandi08@gmail.com, meghanakuriyan27@gmail.com, a.nareshkumar@gmail.com

Abstract - One of the main tasks in Natural Language Processing, Named Entity Recognition (NER), is to recognize and categorize important entities from unstructured text, including people, places, organizations, and different phrases. Conventional NER systems that rely heavily on manual feature engineering, have weak generalization, and have limited contextual understanding.These systems are based on rule-based and statistical learning techniques.In this study, a Named Entity Recognition system using deep learning with Bidirectional Encoder Representations
from Transformers (BERT) model was developed to overcome these drawbacks. The suggested model learns rich contextual representations of words and the tokens that surround them by utilizing BERT's bidirectional self-attention mechanism. Using the BIO tagging technique and WordPiece tokenization with appropriate label alignment for subword units, the model is refined on the CoNLL-2003 benchmark dataset. Hugging Face Transformers and PyTorch are used to build the system, and the seqeval package is used to calculate entity-level precision, recall, and F1-score to assess its performance.Experimental results on the CoNLL-2003 benchmark dataset show that the fine-tuned BERT model achieves an F1-score of approximately 94percent,demonstrating strong performance for transformer-based NER systems.The research results show that transformer-based systems provide better scalability and accuracy and operational resilience for actual NER systems used in intelligent text mining and document analysis and information extraction.

keywords - Named Entity Recognition (NER), Natural Language Processing (NLP), BERT, Transformers, CoNLL-2003, BIO Tagging, WordPiece Tokenization, Token Classification, Deep Learning, Contextual Embeddings, Information Extraction.

ISBN:

PAPER ID: 199

DEVELOPMENT OF AI POWERED DRIVER EMOTION RECOGNITION AND ACCIDENT PREVENTION SYSTEM

Dr. Thaj Mary Delsy T, Karuturi Varshitha, Kagita Sappira
Department of Electronics and Communication Engineering
Sathyabama Institute of Science and Technology
Chennai, India
delsykennedy@gmail.com, karuturivarshi@gmail.com, lenikagita@gmail.com

Abstract – Road accidents caused by driver fatigue, stress, and emotional imbalance pose a significant threat to road safety. While existing systems primarily monitor external factors, they often fail to assess the driver's internal cognitive and emotional state. This paper presents an AI-powered driver monitoring system that integrates real-time facial landmark detection, Eye Aspect Ratio (EAR), Mouth Aspect Ratio (MAR), head pose estimation, and Convolutional Neural Network (CNN)-based emotion recognition.

The system utilizes hardware components such as a buzzer, vibration module, and LED indicators connected via Arduino to provide immediate alerts. It is capable of detecting drowsiness, yawning, stress, anger, and inattentive behavior with high accuracy, even under varying lighting conditions.

Experimental results demonstrate that the proposed system achieves high accuracy and rapid response time, making it suitable for real-world deployment to enhance road safety and reduce accident risks.

Keywords – CNN, EAR, MAR, Artificial Intelligence, Accident Prevention.

Rule-Based Multi-label Soft Skill Prediction System using Resume and SOP Documents

Mohana B[1], M.K. Vidyalakshmi[2]
[12] Department of Data Science & Computing Technologies
SRM Institute of Science and Technology
Kattankulathur, Chengalpattu Dt, Tamil Nadu, India
Email:
b.mohanabaskar@gmail.com, lndivadiyalm1@srmsist.edu.in

Abstract - This research presents a rule-based automated soft skill prediction system that analyzes candidate resumes and Statements of Purpose (SOP) using a web-based application. The system is implemented using the Flask framework and supports user authentication, document upload, and automated processing. Uploaded documents are parsed to extract textual content, which is then cleaned and normalized through preprocessing techniques. The system evaluates the processed text using a rule-based scoring mechanism that identifies the presence of soft skills such as leadership, teamwork, communication, problem-solving, adaptability, and time management. Each skill is assigned a confidence score based on textual indicators detected in the documents. The predicted results are stored in a relational database and presented through a visual interface along with downloadable PDF reports. The system demonstrates a practical and scalable approach for automated soft skill evaluation without requiring labeled training datasets or complex machine learning models.

Keywords — soft skill prediction, resume analysis, NLP, document processing, candidate profiling, automated evaluation

CIRF-IVC-ADSC 2026 - Track 2:

Cybersecurity, IoT & Smart Systems

Covert Communication in Devanagari Script Using Font-Based Text Steganography

Mohd Kamil, Hitesh Singh, Aditee Mattoo
Department of CSE(MTech Integrated) Noida Institute of Engineering and Technology, Greater Noida, India
mohdkamil439529@gmail.com, hitesh.singh@niet.co.in, aditeemattoo@niet.co.in

Abstract – Text steganography based covert communication is difficult because of text rendering instability, font replacement and use of optical character recognition (OCR). The issues are aggravated when it comes to complex writing systems like Devanagari script which uses ligatures, diacritics and special glyphs. In this paper, a font based text steganography scheme of the Devanagari script is described where the font resource is the hidden communication channel. The suggested solution uses deterministic coding into font metadata tables and does not need OCR or document structure or visual representation. Glyph level variants that are controlled so as to maintain perceptual readability are also studied. The system has the highest accuracy of secret message recovery (100 percent under font-preserving conditions) and also has the capability of embedding multiple thousand characters, with no noticeable visual alteration in the rendered product. Quantitative assessment on correctness, determinism, embedding capacity, encoding time and resilience to various transformation conditions are given. There is also a comparison with the known steganography techniques and a discussion of the issue of security, limitations, and future prospects. The findings establish font-internal mechanisms as a sound and consistent medium used in covert communication during text steganography using scripts.

keywords – Covert Communication, Text Steganography, Font-Based Data Hiding, Devanagari Script, Font-Internal En coding.

Automated Reconnaissance and AI-Based Vulnerability Summarization System

Prof. Archana Salaskar , Sakshi Bansode, Devesh Naik, Girish Patil, Aniket Paste
Dept. of Information Technology,Vasantdada Patil Pratishthan's College of Engineering, Mumbai, India

Abstract - In the current cybersecurity landscape, reconnaissance detection has become increasingly important. Still it remains a time consuming and complex process. Existing analysis tools are often not advanced enough to properly handle large volumes of raw data. They struggle to extract meaningful reconnaissance related information. In addition, most security tools focus on detection after the system is attacked. They have not adopted a proactive approach. As these limitations remain, organizations often struggle to detect reconnaissance activities within their infrastructure. This makes them more vulnerable to cyber threats. To address this issue there is a need for an automated system that can identify reconnaissance activities and provide insights across various aspects in a report format that is understandable even to non-technical users. This paper proposes an automated reconnaissance detection system that integrates multiple cybersecurity tools to provide improved awareness and security assessment at an early stage. The system incorporates a chatbot based interface. It guides in identifying vulnerable areas in the infrastructure or system and generates summarized reports. It also provides recommended mitigation measures to improve overall security. The proposed system reduces user effort by eliminating the need to visit multiple security tools sites or applications separately, as it combines reconnaissance and analysis functionalities into a single automated workflow. This integration reduces the time and difficulty level of the detection process. It provides early stage security checks that are accessible and understandable to both technical and non- technical users. It provides proactive defense instead of post attack remediation.

Keywords - Legal AI, Retrieval-Augmented Generation, Large Language Models, Indian Law, Responsible AI, Gemini

A Scalable Deep Learning-Based Intrusion Detection System for Real-Time Cybersecurity in IoT Networks of the Sugar Industry

Ramalakshmi Alagarsamy - Research Scholar, Dr Arockia Edwin Xavier. S - Associate Professor
Department of Electrical and Electronics Engineering, Thiagarajar College of Engineering, Madurai, Tamilnadu, India
ramseee2017@gmail.com, saexeee@tce.edu

The increasing integration of IoT-enabled systems in the sugar industry has enhanced operational efficiency but also exposed critical infrastructures to cyber threats. This paper presents the design and implementation of a scalable, real-time Intrusion Detection System (IDS) using deep learning-based Stacked Ensemble models, including CNN-LSTM, AE-RF, XGB-DNN and LSTM-Bagging, to detect and mitigate severe cyber attacks such as DDoS, Ransomware and Man-in-the-Middle(MITM). The IDS monitors operational parameters like temperature, pressure, energy consumption and flow
across key divisions of the sugar manufacturing process, including Cane Milling, Cane Preparation, Cane Handling, Power Conversion and Bagasse Conveying systems. The proposed system classifies attack patterns and anomalies with high accuracy, precision, recall and F1 score. It is designed to operate efficiently in large-scale, resource-constrained IoT environments. Furthermore, automated threat mitigation strategies ensure minimal disruption to industrial processes. The results demonstrate the IDS's effectiveness in safeguarding IoT networks in the sugar industry by promptly identifying and addressing critical cyber threats.

Keywords
IoT Security, Intrusion Detection System, Sugar Industry, Cybersecurity, Deep Learning, Real-Time Detection, Anomaly Mitigation

An Intelligent Framework for Multi-Lingual Cyberbullying Detection Using XLM RoBERTa

Meghana Y - Master of Technology , Dr. Prathibhavani P M - Assistant Professor
Department of CSE, University Visvesvaraya College of Engineering
Bengaluru, India
ymeghanay@gmail.com, prathibhavani.pm@uvce.ac.in

Abstract - The rapid growth of user-generated content on social media platforms has increased the prevalence of harmful and abusive text, making automated cyberbullying detection a critical research challenge. This study presents a multilingual binary text classification framework for identifying bullying and non-bullying content using the XLM-RoBERTa transformer model. The approach is evaluated on a curated multilingual dataset containing approximately 65,000 text samples across multiple languages. Text preprocessing techniques, including normalization and noise removal, are applied to enhance data quality. The model is fine-tuned using a class-weighted loss function to mitigate class imbalance and trained under a stratified five-fold cross-validation scheme to ensure reliable evaluation. Performance is assessed using accuracy and weighted average F1-score to provide balanced measurement under imbalanced class distributions. Experimental results indicate stable and consistent performance across validation folds, demonstrating the effectiveness of multilingual contextual representation learning for cyberbullying detection. The proposed framework supports scalable automated content moderation in multilingual social media environments.

keywords - Multilingual Text Classification, Cyberbullying Detection, XLM-RoBERTa, Natural Language Processing, Transformer-Based Models, Binary Text Classification, Social Media Content Analysis.

TG-BOT: An AI-Powered Conversational Assistant for Telangana's Agricultural Schemes

Suraj Pullapamtula, Pinnenti Santosh Babu, K. Kiran Prakash
Department of Computer Science and Engineering
Chaitanya Bharathi Institute of Technology
Hyderabad, Telangana, India
ugs22056cse.suraj@cbit.org.in, ugs22055cse.santosh@cbit.org.in,
kiranprakashcse@cbit.ac.in

Abstract— In recent times, access to accurate and timely information about government agricultural schemes has become a significant challenge for farmers in Telangana due to unstructured, incomplete, and multilingual data sources. This paper presents TG-BOT, an AI-powered conversational assistant designed to bridge this information gap using a Retrieval-Augmented Generation (RAG) architecture.

The proposed system consolidates government agricultural documents, including PDFs, circulars, and web-based resources, into a unified and reliable knowledge base consisting of 473 documents. A robust data ingestion pipeline is developed to extract, clean, and preprocess unstructured data, which is then divided into 34,237 semantic chunks. These chunks are indexed using the BAAI/bge-m3 multilingual embedding model, enabling accurate cross-lingual information retrieval.

TG-BOT ensures that the Qwen 2.5 3B Large Language Model (LLM) generates accurate and non-hallucinatory responses by grounding outputs in verified contextual data through strict prompt augmentation. The system supports native multilingual interaction, particularly in Telugu, effectively addressing regional language barriers.

Experimental results demonstrate that TG-BOT is a reliable and efficient tool for supporting Telangana's agricultural community by improving access to relevant government scheme information.

CIRF-IVC-ADSC 2026 | ISBN: 978-81-999525-0-8

An ESP Mesh based IOT System for Smart Agriculture

Dr. S Deepak Raj - Associate Professor, Kruthika R Reddy, Marlakunta Chinmayee, Meghana K M
Dept. of Information Science and Engineering, Nitte Meenakshi Institute of Technology
Bengaluru, India
deepak.raj@nmit.ac.in, 1nt22is079.kruthika@nmit.ac.in, 1nt22is091.marlakunta@nmit.ac.in, 1nt22is079.meghana@nmit.ac.in

Abstract - Smart agriculture increasingly depends on distributed, high-resolution sensing systems capable of capturing real-time soil and environmental dynamics with minimal infrastructure and cost. Conventional wireless sensor networks, however, often face limitations in scalability, energy efficiency, and network robustness, particularly in fragmented agricultural landscapes where connectivity is inconsistent. This work presents an ESP-based mesh IoT architecture designed to enable resilient, self-organizing, and low-cost monitoring of critical agronomic parameters. The system integrates a multi-node mesh network for distributed soil sensing, a gateway-assisted cloud uplink for remote accessibility, and a unified dashboard for visualization, alert generation, and long-term water-footprint assessment. By leveraging a decentralized mesh topology, the framework ensures reliable propagation of sensor data across dynamically changing link conditions, while cloud integration facilitates continuous supervision and early-warning capabilities for irrigation and soil-health anomalies. Experimental evaluation of the prototype demonstrates stable multi-hop communication, consistent sensing performance, and seamless end-to-end data flow from field nodes to the user interface. The results highlight the potential of ESP- based mesh networks as an accessible and scalable digital infrastructure for precision agriculture, supporting improved resource efficiency and informed agronomic decision-making.

keywords - Smart agriculture, Internet of Things (IoT), wireless sensor networks, mesh networking, ESP32, cloud-based monitoring, soil sensing, precision irrigation.

PhishGuard: A Hybrid Deep Learning Ensemble with Active Learning for Real-Time Gmail Phishing Detection

DR .SARAVANAN.S - Assistant Professor, BATHALA PUNEETH & REDDY JOSHMA BHARATHI - UG Student
Department of CSE
Vel Tech Rangarajan, Dr.Sagunthala R&D Institute of Science and Technology
Avadi, Chennai,
dsaravanan@veltech.edu.in, vtu22553@veltech.edu.in, vtu21781@veltech.edu.in

Abstract – Phishing attacks remain the leading vector for cybercrime because they exploit human trust while overcoming conventional security systems. The researchers developed Phish-Guard as an enhanced system which detects phishing attacks through client-side real-time detection. The system upgrades from a standard Random Forest classifier system through its Hybrid Deep Learning Ensemble model which combines CNN-BiGRUAttention for structural pattern recognition with DistilBERT transformer for semantic analysis. The system achieves high accuracy while eliminating false positives through its use of Sender Domain Trust Signal and Active Learning feedback loop. The solution uses FastAPI service to analyze messages received in the past 24 hours because this approach helps maintain fast operational performance. The system achieved its highest performance with an F1 score of 0.9933 and operational latency of approximately 200 milliseconds which confirmed its potential for proactive client-side security.

Keywords – Phishing Detection, Deep Learning, BERT, CNN-BiGRU, Active Learning, Chrome Extension, FastAPI, Gmail API, Cybersecurity.

Advanced Intelligent Database Frameworks for Yield Enhancement in Semiconductor Fabrication

Padmaja Pulivarthy[1], Anji Reddy Erugula[2]
[1] Senior Software Engineer, Samsung
IT Infrastructure, Austin, Texas, USA
p.pulivarthy@samsung.com
[2] Principal Software Engineer / Architect, CommScope
ANS Engineering, CNS, Bangalore, Karnataka, India
anji.erugula@commscope.com
ORCID ID: 0009-0006-4532-9362

Abstract -Semiconductor fabrication process is a complicated activity and entails intricate operations with noisy sensor information of high-dimensionality, and fault detection and yield enhancement is complicated. The conventional rule-based monitoring systems and statistical process control (SPC) methods are not effective to address these complexities and frequently results in the unnoticed process variations and massive loss of yield. This study introduces a machine learning-based system to predict faults and improve yield, and these issues are handled in this study through a smart, data-driven framework. The system architecture will comprise of a data ingestion module, preprocessing and feature handling module, machine learning engine and prediction and decision-support module. Data used: Semiconductor manufacturing sensor data of a benchmark data set with multivariate process data, high-dimensionality, missing data, binary quality data (pass/fail), and so on. The preprocessing module deals with the missing values, normalization, scaling and feature selection. The machine learning engine uses the classifiers of Random Forest and XGBoost, model training, hyperparameter optimization, and techniques of dealing with class imbalance. Fault prediction method is step-by-step method which entails reception of data, preprocessing, model training, fault prediction, and yield-related insights generation. The yield enhancement decision module takes the prediction as its input and takes high-risk cases to give feedback on fine-tuning processes and preventive maintenance, and finally gives the recommendations to enhance the yield. It has been demonstrated that the suggested framework is superior in comparison with the traditional techniques and helps improve the accuracy of fault detection and promote the yield rate.

Keywords: Fault prediction, yield enhancement, machine learning, semiconductor fabrication, process data, XGBoost, Random Forest.

Android Asset Encryption with Runtime Decryption Using White-Box Cryptography and Virtualized Key Protection

Karthik D, Mahibalan S, Sreedevi B
Department of ECE, St. Joseph's Institute of Technology
Chennai, TamilNadu, India
karthiksiky@gmail.com, mahibalan798@gmail.com, sreedevib@stjosephstechnology.ac.in

Abstract - The security of digital assets within Android applications is a critical concern for developers, as the open nature of the Android ecosystem makes reverse engineering straightforward. Traditional protection methods, including hardcoding Advanced Encryption Standard (AES) keys within Java source code, obfuscating with ProGuard, and even implementing encryptionlogic in native code, have proven ineffective against modern static analysis tools and dynamic instrumentation frameworks like Frida. Cryptographic keys remain vulnerable to extraction within seconds through Java Cryptography Architecture (JCA) API hooking, memory dumping of native heaps, and inline hooking of JNI functions, as current implementations fail to adequately protect key material during runtime operations. This paper proposes a novel, robust framework that addresses these vulnerabilities through a dual-layer protection mechanism integrating White-Box Cryptography (WBC) with custom Virtual Machine (VM) protection. Our solution employs AES-256 for asset encryption and runtime decryption, while protecting the AES-256 key through a dual-layer approach: first, by embedding it within white-box cryptography, and second, by obfuscating the decryption logic using a custom virtual machine opcodes.
This hybrid architecture, implemented in a native C++ library, ensures that the key never appears in memory in plaintext form. The system implements automated asset encryption during build time and injects protected decryption routines that transparently replace standard Android AssetManager operations.

Abstract - Mobile Application Security, Asset Protection, White-Box Cryptography, Runtime Protection, Virtual Machine Obfuscation, Reverse Engineering Protection

Intelligent Real-Time Traffic Congestion Monitoring and Prediction System Using Machine Learning

Mr.Kishore Kumar.K,Mr.Jeevanantham.S, Mr.Janakiraman.A.NG - Scholars, Mrs. Gowthami K- Assistant Professor
Department of Data Science and Business Systems
Department of Computational Intelligence
SRM Institute of Science & Technology, Kattankulathur
Chennai, Tamil Nadu, India
dhanasek1@srmist.edu.in, pm5186@srmist.edu.in

Abstract - The rapid urbanization and growing number of vehicles in cities have made traffic congestion a critical issue affecting productivity, energy consumption, and the environment. This paper presents the design and implementation of an Intelligent Real-Time Traffic Congestion Monitoring and Prediction System that integrates Machine Learning (ML) and the Internet of Things (IoT). The system gathers live traffic data using IoT sensors and cameras, processes it through a cloud-based analytical pipeline, and predicts congestion levels using ML algorithms. Results are visualized on a real-time dashboard to help authorities take proactive control actions such as signal optimization and route diversion. The framework aims to enhance road efficiency, reduce travel time, and promote sustainable urban mobility.

Keywords - Traffic Congestion, Machine Learning, IoT, Smart Cities, Real-Time Prediction

Abstract Proceedings of the CIRF International Virtual Conference on AI, Data Science & Cybersecurity (CIRF-IVC-ADSC 2026) March 2026

This Abstract Proceedings volume presents a curated collection of research summaries from the CIRF International Virtual Conference 2026. The conference brings together academicians, researchers, industry experts, and students to explore advancements, innovations, and challenges in the domains of Artificial Intelligence, Data Science, and Cybersecurity.

The contributions included in this volume reflect emerging trends, practical applications, and interdisciplinary approaches that are shaping the future of technology and digital security. Each abstract has been reviewed to ensure quality, relevance, and academic integrity.

This publication serves as a valuable reference for researchers, practitioners, and students, fostering knowledge exchange and encouraging further exploration in these rapidly evolving fields.

Published by:
Computational Intelligence Research Foundation (CIRF)
India

ISBN: 978-81-999525-0-8

Contact Us :

90030 21355

13,Ayanavaram Road, Ayanavaram, Chennai 23

cirf.co.in

9 788199 952508