PROCEEDINGS OF ABSTRACTS

International Conference on

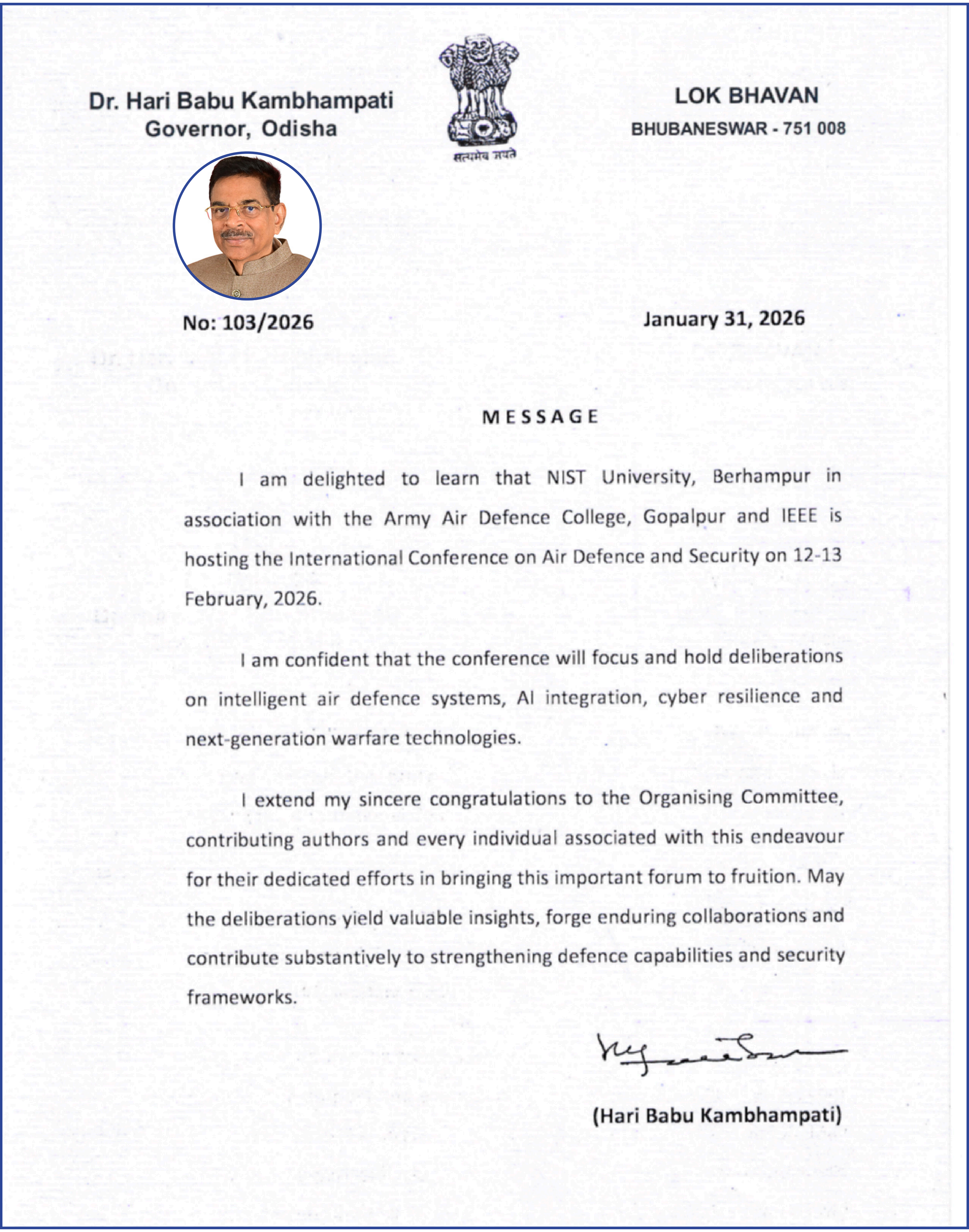
AIR DEFENCE AND SECURITY (ICADS-26)

Organised By

Army Air Defence College
NIST University

12-13th February 2026

Message from the Governor



Dr. Hari Babu Kambhampati
Governor, Odisha

सत्यमेव जयते

LOK BHAVAN
BHUBANESWAR - 751 008

No: 103/2026

January 31, 2026

MESSAGE

I am delighted to learn that NIST University, Berhampur in association with the Army Air Defence College, Gopalpur and IEEE is hosting the International Conference on Air Defence and Security on 12-13 February, 2026.

I am confident that the conference will focus and hold deliberations on intelligent air defence systems, AI integration, cyber resilience and next-generation warfare technologies.

I extend my sincere congratulations to the Organising Committee, contributing authors and every individual associated with this endeavour for their dedicated efforts in bringing this important forum to fruition. May the deliberations yield valuable insights, forge enduring collaborations and contribute substantively to strengthening defence capabilities and security frameworks.

(Hari Babu Kambhampati)

Message from the COAS

सेनाध्यक्ष

CHIEF OF THE ARMY STAFF

The character of warfare is undergoing a paradigm shift. Kinetic engagements are now intertwined with cyber operations, information warfare, electronic warfare, space-based enablers and resilient communications networks. In this environment, especially in the light of Op SINDOOR, superiority in air defence and integrated air missile defence system is imperative to safeguard critical assets and ensure freedom of manoeuvre.

International Conference on Air Defence and Security (ICADS-26) against this backdrop is a timely initiative that aligns with the Indian Army's initiatives of 'Decade of Transformation' and Years of Networking & Data Centricity 2026 & 27, to focus on becoming a technologically empowered, agile and joint force capable of prevailing across the full spectrum of conflict. The partnership between the Army Air Defence College and NIST University, Berhampur is also a fine example of Military Civil Fusion to accelerate innovation and enhance operational readiness of the Indian Army.

The themes and tracks of ICADS-26 ranging from AI/ ML, C41SR systems and autonomous platforms to cyber resilience, aerospace sensors and missile defence address Indian Army's ambitious modernisation pursuits and captures the essence of Hon'ble PM's message of JAI (Jointness, Atmanirbharta and Innovation). Publishing of the peer reviewed IEEE Xplore magazine will ensure that ideas conceived here will evolve to enhance surveillance, decision-support and engagement across the multi-domain battlespace.

On behalf of all Ranks of Indian Army, I convey my compliments to the organisers, partners and delegates for their commitment to strengthen the nation's defence preparedness through rigorous scholarship and practical innovation.

'Jai Hind'

Upendra D

Upendra Dwivedi
General Chief of the Army Staff

Message from the GOC-in-C ARTRAC

The character of warfare in the 21st Century Battlespace is undergoing a fundamental transformation. We are witnessing a paradigm shift where the distinction between peace and conflict has diminished and the battlespace has expanded beyond the physical domains into the cognitive and digital realms. In this era of 'War in Peace', the integration of AI, Cyber Resilience and Next-Generation Warfare is not merely an option; it is an operational imperative.

It is against this backdrop that I view the International Conference on Air Defence and Security (ICADS-26) as a timely & critical intervention. The theme, 'Intelligent Defence : Securing the Future with AI, Cyber, Resilience and Next-Gen Warfare' strikes at the very heart of our future readiness. As the 'Sensor-to-Shooter' loops compress to single-digit minutes and the 'Air Littoral' becomes increasingly contested by diverse threats - from loitering munitions to Hypersonic vectors - our Air Defence architecture must possess the cognitive agility to discern the 'Signal' from the 'noise' and react at the speed of relevance.

The challenges we face - ranging from 'Electronic Fratricide' to the 'Cyber Takeover of Unmanned Systems' - cannot be solved in silos. The 'Integration Imperative' demands a Whole-of-Nation approach. By bringing together the uniformed fraternity with the intellectual capital of our Academia and the technical prowess of our Industry and Start-Ups, ICADS-26 will assist in forging the necessary ecosystem for realistic problem definitions and iterative innovations. The synergy is essential to bridge the gap between user consideration, doctrinal intent and technological capability.

I commend the Army Air Defence College and NIST University for curating this platform. The archival of these proceedings in IEEE Xplore serves not just as a record of academic rigour but a repository of actionable thought, leadership for the wider defence community.

I am sanguine that the deliberations during this conference will transcend theoretical discourse and pave the way for tangible Doctrinal and Technological Roadmaps that will fortify India's Air Defence capabilities and consequently the Security of the Nation. I wish the organisers and all participants; professionally enriching deliberations and a resounding success.

'Akashe Shatrun Jahi'

'Jai Hind'!

Devendra Sharma, PVSM, AVSM, SM
Lieutenant General
General Officer Commanding-in-Chief
Army Training Command

Message from the Commandant, Army AD College

International Conference on Air Defense and Security (ICADS-26), underscores the transformative potential of academia-military collaboration in addressing contemporary security challenges. This landmark event emerged directly from the Memorandum of Understanding (MoU) signed between the Army Air Defence College (AADC), Gopalpur, and NIST University in June 2025, exemplifying how strategic partnerships can yield tangible outcomes in defence innovation.

Under the theme “Intelligent Defense: Securing the Future with AI, Cyber Resilience, and Next-Gen Warfare,” ICADS-26 brought together military officers, researchers, engineers, policymakers, and industry leaders to deliberate on critical domains including AI/ML applications, autonomous systems, electronic warfare, cyber operations, hypersonic threats, and integrated air-missile defence architectures. These discussions bridged operational realities with cutting-edge research, ensuring that solutions are not only theoretically sound but also battle-ready, ethical, and scalable for joint force employment.

For the armed forces, the conference provides actionable insights into multi-domain superiority, human-machine teaming, and resilient C4ISR networks essential for deterrence and decisive victory. Civilian participants gained invaluable perspective on the rigours of defence applications, fostering indigenous capabilities aligned with Atmanirbhar Bharat. The peer-reviewed proceedings, now archived in IEEE Xplore, will serve as an enduring reference for global scholars and practitioners, perpetuating the knowledge exchange initiated here.

AADC remains committed to deepening this MoU-driven synergy with NIST University, translating conference outcomes into training curricula, prototypes, and fielded systems that strengthen India's air defence posture across all threat spectra. The high-quality contributions and robust deliberations reflect the professionalism of all involved.

Congratulations to the delegates, organising committees, and partners for making ICADS-26 a resounding success.

‘Akashe Shatrun Jahi’
‘Jai Hind’!

RC Srikanth, AVSM, VSM
Lieutenant General
Commandant, Army AD College & Senior Colonel Commandant
Corps of Army Air Defence

Message from the DG Army AD

The Corps of Army Air Defence stands at the forefront of safeguarding the nation’s skies against a rapidly evolving spectrum of threats, from legacy aircraft and cruise missiles to unmanned systems and long-range precision weapons. In this context, the International Conference on Air Defense and Security (ICADS-26) is both timely and obligatory.

The Army Air Defence College, Gopalpur, has consistently endeavoured to blend rigorous military training with exposure to cutting-edge technologies in sensors, weapons, networks and simulation. Co-hosting ICADS-26 with NIST University strengthens this effort by bringing in the research depth, engineering expertise and youthful energy of a leading technical institution. Together, these partners provide a unique environment where operational problems can be examined through scientific methods and innovative solutions can be tested against real-world constraints.

The conference’s focus on AI/ML, cyber resilience, C4ISR, aerospace sensors, missile defence and autonomous systems aligns closely with the modernization priorities of Army Air Defence and the wider joint force. Importantly, these discussions will consider not only performance and lethality, but also issues of ethics, resilience, human-machine teaming and training - factors that are critical when lives and national security are at stake.

The publication of peer-reviewed proceedings in IEEE Xplore will ensure that the insights generated here inform practitioners and researchers in India and abroad. The Corps of Army Air Defence expects that many of the ideas discussed at ICADS-26 will, in due course, contribute to more robust, adaptive and integrated air defence capabilities for the Nation.

Warm greetings to all delegates, and sincere appreciation to the organising teams of Army Air Defence College and NIST University for their dedicated efforts.

‘Akashe Shatrun Jahi’

‘Jai Hind’!

Sumer Ivan D’Cunha, PVSM, SM, PhD
Lieutenant General
Director General & Colonel Commandant
Corps of Army Air Defence

Message from the President (NIST University)

As the Patron of the International Conference on Air Defense and Security (ICADS-2026), I have the pleasure of welcoming you to this premier international conference, which is being held at NIST University, Institute Park, Berhampur, Odisha on February 12-13, 2026.

With rapid advancement of communication, computing and technologies the typical conventional warfare is becoming obsolete and seems no more effective and relevant. There is a foundational shift in modern military doctrine to achieve strategic objectives using advanced technologies. Modern warfare is no longer limited to the battlefield alone. Among other options, it can be fought in many ways like: Cyber Warfare, Information Warfare, Use of Autonomous Systems etc. This is the inaugural year of the conference which witness it as a high quality forum for thought leaders, policy makers, scientist and engineers to present their latest finding in this rapidly changing field of Air Defense and Security. The largest number of paper submissions covering a much broader spectrum is a testimonial to the growing interest in this conference. In addition to the paper presentations, ICADS-2006 features distinguished keynote speakers and tutorials. I would like to convey my sincere thanks to Dr. Ali Yuce, Dr. Noor Zaman Jhanjhi, Shri G. C. Pati, Dr. Anshuman Roy, Mr. Vijay Sutrakar and many others , those have accepted our invitation to give the keynote lecturers. A distinct feature of this conference is the exhibition by many leading organizations in the field of air defense and security in general. I greatly appreciate the sponsor Defense Research Development Organization (DRDO) for their generous financial contribution and support. The conference is the result of the hard work of contributing authors, reviewers, and conference committee members. I am grateful to all these people specifically all the conference chairs for making the conference a grand success.

Finally, I would like to thank you, the participants, whose interest is the reason for the existence and success of this conference.

Mohapatra

Dr. Sukant K. Mohapatra
President, NIST University
Patron, ICADS-26

Message from theVice Chancellor (NIST University)

It is my great pleasure to welcome you to the inaugural International Conference on Air Defense and Security (ICADS-26), centered on the theme of intelligent air defence, cyber resilience, and AI-driven innovations for security.

The global security landscape is undergoing a seismic shift. The rise of AI, autonomous systems, and electronic warfare is reshaping not only defense capabilities but the strategic paradigm itself. These challenges demand exceptional agility and integration across defence and academic ecosystems. In this context, I deeply appreciate the academic and institutional partnerships that I was privileged to facilitate in strengthening this conference.

The response to ICADS-26 has been strong; we received over 350 submissions from across the globe. Following a meticulous peer review process, approximately 20% were selected for presentation, ensuring a program of high academic and technical rigour and reflecting the vanguard of contemporary defence research.

The Indian Union Budget for 2026–27 has underscored defence modernisation through increased capital investment in advanced systems. This focus on technology infusion and operational readiness closely aligns with the core pillars of ICADS-26. Accordingly, the conference is more than a forum for presenting papers; it is an opportunity to build enduring bridges between ideas, experience, and practice.

To our young researchers, your technical creativity is driving the next wave of innovation from AI-enabled decision systems to resilient cyber architectures. Equally indispensable is the engagement of seasoned professionals and defence leaders, whose stewardship ensures that innovation remains grounded in operational realities and guided by strategic acumen.

This souvenir captures more than abstracts and messages; it reflects the collective commitment of the ICADS community to advancing knowledge that informs defence strategy, strengthens security architectures, and supports resilient national institutions.

I congratulate all authors, national and international speakers, participants, reviewers, sponsors, and organisers on the success of ICADS-26. Kudos to the team for producing a fine conference compendium. May the learning and partnerships forged here have a lasting impact.

With best wishes for a successful and inspiring conference,

Prof. Priyadarsan Patra
Vice Chancellor, NIST University; Patron, ICADS-26

Message from General Chairs

The evolving nature of air defence and security reflects a broader transformation in warfare, where speed of decision-making, intelligent systems and seamless integration across domains are as decisive as platforms and firepower. Addressing these challenges requires sustained dialogue between the armed forces, academia, research institutions and industry grounded equally in operational realities and technological foresight. The International Conference on Air Defence and Security (ICADS-26) jointly organized by Army Air Defence College & NIST University on 12 & 13 February 2026, has been conceived precisely with the above mentioned objective. As the inaugural edition, ICADS-26 marks a significant milestone in structured collaboration between the Indian Army and academia, providing a credible international forum for examining emerging threats, future capabilities and innovative solutions across the defence and security spectrum. It has been our privilege to serve as General Co-Chairs for ICADS-26. We place on record our deep appreciation for the dedication and professionalism of the organizing team, partners, reviewers, speakers and delegates whose collective efforts have shaped this conference into a meaningful platform for collaboration and progress. We are confident that ICADS-26 will contribute enduring value to the discourse on air defence and help catalyze ideas that translate into strengthened national capability.

Jai Hind!

Dr. P Rajesh Kumar
Dean of Academics
NIST University, Odisha

Col Manoj Kumar Yadav
Col Instructor, Science & Tech Wing
Army AD College

G Ramesh
Indian Space Research
Organisation (ISRO)

Message from Programme Chairs

It gives us immense pleasure that the International Conference on Air Defense and Security (ICADS-26) is being held during 12-13th February 2026, jointly organized by the NIST University and Army Air Defence College, Gopalpur. The overwhelming response to the conference is a strong reflection of the growing importance and relevance of research in the areas of air defense, security systems, and allied technologies.

ICADS-26 received over 350 research paper submissions, addressing a wide range of theoretical and applied aspects aligned with the conference theme. After a rigorous peer-review process, only 58 high-quality papers have been selected for presentation in the conference. This highly selective acceptance underscores the technical depth, originality, and relevance of the papers to the theme of the conference.

The conference brings together researchers, academicians, defense experts, industry professionals and practitioners to share insights, exchange ideas, and discuss emerging challenges and innovations in the domain of air defense and security. The technical program includes keynote addresses by distinguished experts, technical paper presentations, and exhibitions, offering opportunities for scholarly interaction, research collaboration, and knowledge dissemination.

We extend our sincere appreciation to the authors for their valuable contributions, the reviewers for their diligent efforts, and the technical program committee for their dedicated support in making ICADS-26 a success. We are confident that the deliberations during the conference will foster meaningful interaction and future collaboration in the field of air defense and security.

We wish all participants a stimulating and rewarding conference experience.

Prof. Manas R Patra
NIST University

Lt Col DK Sahu
Army AD College

Prof. Shaik Rafi Ahamed
IIT Guwahati

Organisation Committee

Patrons

Prof. Priyadarsan Patra
Vice Chancellor, NIST University

Dr. Sukant K Mohapatra
President, NIST University

Brig. (Dr.) L C Patnaik
Ex Chairman, OPSC

General Chairs

Dr. P. Rajesh Kumar
Dean of Academics

Col MK Yadav
Army Air Defence College

G Ramesh
ISRO

Program Chairs

Dr. Manas R. Patra
NIST University

Lt Col DK Sahu
Army AD College

Prof. Shaik Rafi Ahamed
IIT Guwahati

Finance Chair

Dr. Bishnukar Nayak
NIST University

Organisation Committee

Sponsorship Chair

Dr. Sandipan Mallik
NIST University

Exhibit Chair

Dr. Sushanta K Sahu
NIST University

Publicity Chairs

Dr. Brojo K Mishra
NIST University

Maj Pranjal Agarwal
Army AD College

Capt Ayush Mudgal
Army AD College

Publications Chairs

Dr. Ratikanta Nayak
NIST University

Maj Shubham Shakya
Army AD College

Organization Chairs

Dr. Sasmita Padhy
NIST University

Dr. Preeti Ranjan Sahu
NIST University

CONTENT

Content

1. Conference Overview 06
2. Organising Institution: NIST University 07
3. Co Organizing Institution: Army Air Defence College 08
4. Invited Dignitaries & Keynoters 09
5. Program Agenda :
International Conference on AIR DEFENCE AND SECURITY (ICADS-26) 13
6. Abstracts

1. Enhancing AI-Powered Cyber Defense: An Explainable and Resilient Framework for Future Intelligent Warfare 15
2. AI-driven battlefield decision support using probabilistic threat modeling (Bayesian Networks) integrated with multi-objective optimization (NSGA-II) 16
3. Deep Learning Essence in XSS and CSRF 17
4. A Novel Framework to Convert Public Source URLs to Cryptographic-enabled API Key 18
5. Analyzing the Impact of LOS and NLOS Propagation on Underwater Localization Accuracy Using Data Collected by Autonomous Underwater Vehicles (AUVs) 19
6. Practical Implementation of Dubins Method for Path Planning of Fixed-wing UAV using Genetic Algorithm 20
7. Rotation-Dependent RCS Signature Analysis and Machine-Learning-Based Identification of a Chipless RFID Tag for Passive Defence Sensing Applications 21
8. Adversarial Robustness in LLMs: A Survey of Attacks and Defenses with Experimental Evaluation of Decision Based Attack and Human-in-PipelineDefense 22
9. Adversarial Robustness and Explainability in Intrusion Detection Systems: Maintaining XAI Integrity Under Adversarial Attacks 23

Content

10. Post-Quantum Cryptography using CRYSTALS-Dilithium on Application of Defense Security Systems 24

11. Implementation of Securing Text Data Using Steganography and Cryptographic Techniques 25

12. XenoCipher : A Secure Key Exchange and Encryption Model for Data Protection 26

13. LLM-Based Agentic Decision Support for Maritime Threat Assessment 27

14. Smart Autonomous Surveillance Rover (SASR) 28

15. EdgeWise Pretrain: Few-Shot Graph Intrusion Detection for Heterogeneous Networks 29

16. Spectral Attention GNN Framework for Secure Telemetry in UAV and Satellite Communication Systems 30

17. Hybrid Orthogonal CNN–ResNet50 with Grey Wolf Optimization for Malware Classification on MalNet 31

18. Privacy-Preserving Collaborative Threat Intelligence for Predictive Cyber Defense 32

19. Quantum-Enhanced Blockchain for Optimized Supply Chain Management: Leveraging QAOA and Secure Transaction Protocols 33

20. Smart Cybersecurity: A Dataset-Driven Comparative Analysis of ML Techniques for Network Intrusion Detection and Prevention 34

21. NeuroMesh Sentinel: A Decentralized Swarm Intelligence Framework for Autonomous Multi-Cloud Security Through Distributed Consensus and Behavioral Biometrics 35

22. Hybridization of Meta-Heuristic based Optimization Techniques with RNN- based Machine Learning for Detection of Cyber attacks 36

Content

23. A Dual-Model NIDS Architecture Combining Convolutional Neural Networks and Autoencoders for Robust Attack Detection 37

24. Geospatial Crime Type Prediction Using Machine Learning 38

25. Design of an IDS for Detection of Adversarial Attacks in IoT using Machine Learning 39

26. ML and Cloud-Based Turbulence Prediction Model for Aviation Safety 40

27. Variance-Guided Adaptive DWT–DCT Image Steganography for Defense and UAV Applications 41

28. Sensitive Data Masking And Security Validation In File Upload System 42

29. An Explainable WGAN-GP Framework for Deepfake Voice Detection 43

30. Quantum-Resistant Cryptography for Secure IoT Communication Systems 44

31. A Miniaturized Frequency Reconfigurable Antenna for Sub-6 GHz 5G and WBAN Communications 45

32. Military Digital Twins - A Data-hardened Architecture for Digital Twins to Enable Operational Resilience in Adversarial Environments 46

33. Detection of Coordinated Social Media Manipulation Using Temporal Network Analysis 47

34. Strategic Information Confrontation Through Persistent Digital Surveillance: An Integrated OSINT-Social Engineering Framework for Long-Term Intelligence Weaponization 48

35. Transforming Text into Secure Information: A DES Encryption and Deep Learning Approach 49

36. Quantifying Narrative Dominance: The “Authenticity Trap” and Data-Driven Decision Support in Cognitive Warfare 50

Content

37. Learning-Driven Wi-Fi Intrusion Prevention Using Anomaly Detection and Attack Classification 51
38. SAKSHI: Agentic AI for Regional Intelligence using Structured Open-Source Intelligence (OSINT) 52
39. LSTM based Threat Intelligence Methods for Intrusion Classifications of DOS Attack in WSN 53
40. A Real-Time Drone Detection System using Hybrid Deep Learning YCFANet 54
41. Operation Sindoor: Role Of The Indigenous Integrated Air Command And Control System (IACCS) In A High-Tempo Network Centric Conflict: A Case Study 55
42. Platform Power and National Security Doctrine 56
43. Study of Propellants for Muzzle Velocity Enhancement in Medium Caliber Gun Ammunition 57
44. Passive Detection System: De-Novo 58
45. Electronic Fratricide in Air Defence Operations While Countering UAS In Tactical Battle Areas 59
46. Sensitivity Enhancement of Quantum Radar Using Entangled Single Photon Source for Military Defense Security 60
47. Niche and Disruptive Technologies in Defence & Security 61
48. AI-Based Resonance Avoidance in Military Vehicle Components 62
49. Cyber Takeover of UAS - Opportunities & Challenges 63
50. Air Littoral Emerging Concept for Land Forces 64
51. DRAMS : Threat & Role of Ground Based Air Defence Weapon System 65
52. Evolving Air Threat : Impact of Technological Upgrades in Field of Avionics, Sensor to Shooter Linkages, BVR & Stand Off Capabilities and Extensive Proliferation of UAS 66
53. Strategic Environment and Geopolitical Shift - Artificial Intelligence, Cyber Resilience and the Architecture of Air and Missile Defence in 2026 67

Content

54. Technological Innovation & Future Security Impact of Supersonic and Hypersonic weapon Systems on Air and Missile Defence 68

55. Multi-Sensor intelligence fusion for real-time airspace security 69

56. Battlefield 2035: Emerging Contours, Adversarial Postures and Implications for India’s Capability Development 70

57. Agentic Geo-Intelligence-Based Spatio-Temporal Operational Risk Analysis in Sensitive Regions 71

Conference Overview

The International Conference on Air Defense and Security (ICADS-26) is envisioned as a flagship interdisciplinary forum designed to address the rapidly evolving challenges of global defense and security in an era defined by technological disruption and geopolitical complexity. Built around the theme “Intelligent Defense: Securing the Future with AI, Cyber Resilience, and Next-Gen Warfare,” ICADS-26 aims to foster deep intellectual exchange at the intersection of advanced research, emerging technologies, operational practice, and policy formulation. The conference seeks to unite a diverse community of researchers, scientists, technologists, industry leaders, entrepreneurs, defense professionals, and policymakers to share insights, explore solutions, and collectively shape the future of defense and security. The inaugural edition of ICADS-26 will be held on 12–13 February 2026 at NIST University, and is jointly organised by NIST University and the Army Air Defence College, Gopalpur, Berhampur. This academic–military collaboration reflects the conference’s vision of bridging theory and practice, innovation and deployment, and research and real-world operations. By bringing together stakeholders from academia, government, strategic institutions, and industry, ICADS-26 aims to promote collaboration, inform evidence-based policy, and accelerate innovation across critical defense domains.

Additional focus areas include smart sensor networks, integrated battlefield intelligence, quantum technologies for defense, electronic warfare and electromagnetic spectrum dominance, and the role of 5G and next-generation connectivity in enabling resilient, network-centric defense systems. Recognizing that technology operates within human, organizational, and institutional contexts, ICADS-26 devotes attention to human factors, leadership, and policy dimensions. Topics include psychological resilience in modern warfare, national and global defense policies, advanced training using simulation and AR/VR technologies, human–machine teaming in combat and decision-making, and leadership under high-stress conditions. The expanding arena of cyber and information warfare forms another pillar, encompassing cybersecurity strategies, threat intelligence, offensive and defensive cyber operations, information superiority, social media manipulation, psychological operations, and cognitive warfare. Through this agenda, ICADS-26 aspires to contribute meaningfully to the development of secure, intelligent, resilient, and ethically grounded defense ecosystems for the future.

Organising Institution: NIST University

The NIST University (www.nist.edu), Institute Park, Berhampur, Odisha, India, was established in 1996. Then, it was the vision and dream of the founding members to have NIST as a center of academic and research excellence at par with International Research Universities in their home state of Odisha, India. Nestled in the green hills of Pallur, the campus is spread over 65 acres with world class academic infrastructure, halls of residence, sport complex and other facilities. The campus has a green canopy made of 45 types of native and decorative flora which is home to more than 28 types of fauna.Today, NIST is a premiere research university in the country offering undergraduate, graduate, and Ph.D. programs. NIST has always been re-imagining and transforming, with rigorous and ever-evolving academic programs to meet future needs by outstanding teaching, pioneering innovation, and research programs that foster global partnership. NIST has set benchmarks through its outstanding academic programs, quality education, and cutting-edge multidisciplinary research. NIST has various state of art laboratories and research facilities in computing, communication and sciences. Leveraging its global collaboration and partnership with industries and top universities and research labs around the world, NIST has embarked on the journey in establishing Global Innovation Centers (GICs) in areas like 5G and Future Communications, Semiconductors using advanced material, Artificial Intelligence (AI) and Biotechnology etc. GICs are expected to carry out extensive applied research and create technology hubs leveraging research and innovation at NIST.

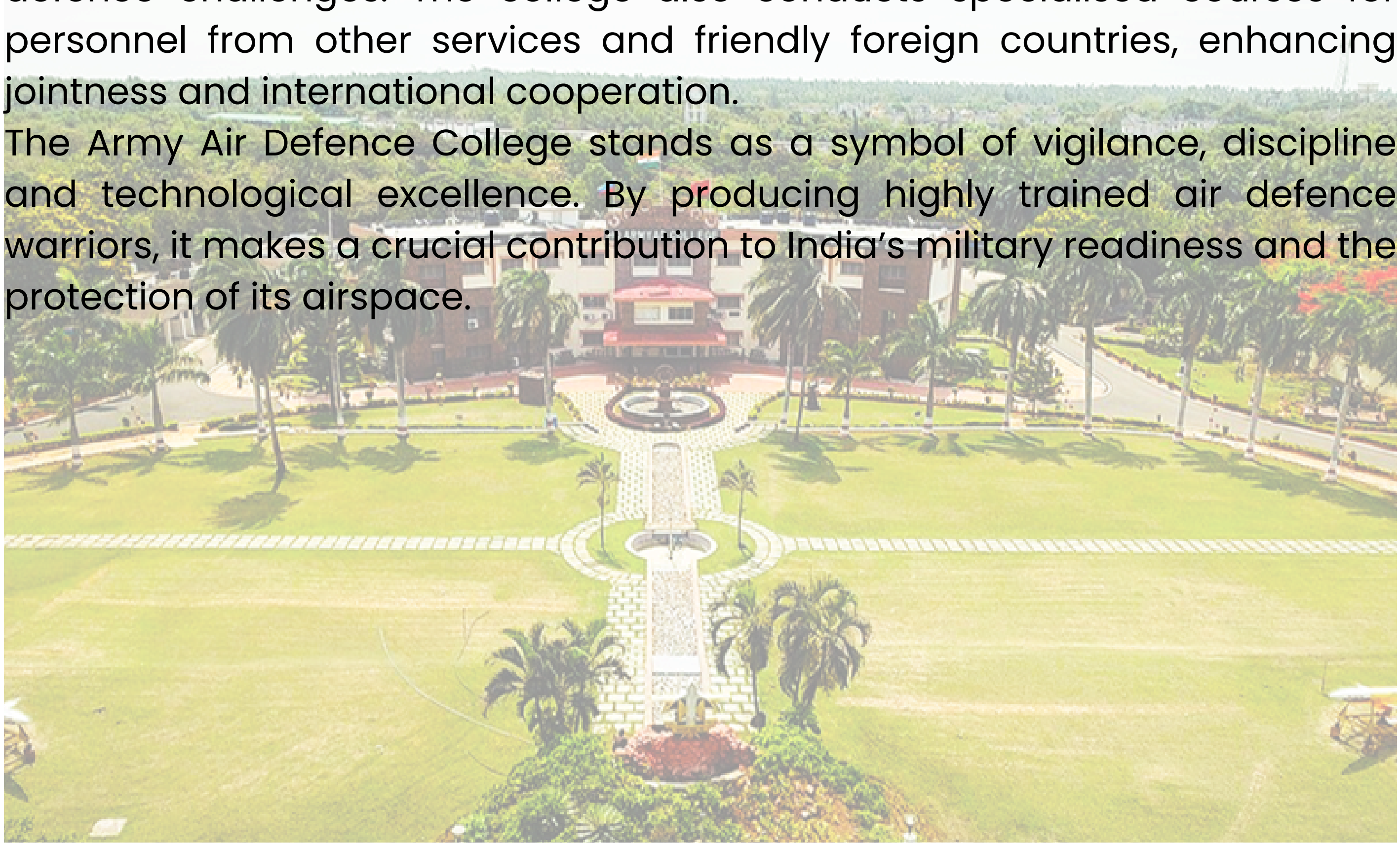
NIST faculties are among BOYSCAST and Fulbright scholars, INSA fellows, USRI scientist award recipients including other achievements. NIST has research collaborations with many Universities around the globe and has strong industry-academia partnership with multiple industries in different sectors. NIST is NACC "A" accredited. Over the years it has been ranked highly in the country by NIRF, (MHRD - Govt. of India), Atal Ranking of Institutions on Innovation Achievements (ARIIA) by (ME - Govt. of India) and other ranking organizations. In 2025 it ranked 28th in the country in engineering by Times Engineering ranking.

Co Organizing Institution: Army Air Defence College

The Army Air Defence College (AADC) is the premier training institution of the Indian Army's Corps of Army Air Defence, located at Gopalpur Military Station, near Berhampur. It plays a vital role in preparing officers and soldiers to protect the nation from aerial threats and to operate advanced air defence weapon systems with precision and professionalism. The college has a rich historical legacy that dates back to the early 1940s, when anti-aircraft training was initiated during the Second World War. Over the decades, it evolved in response to technological advancements and operational requirements. In 1979, the Air Defence and Guided Missile School and Centre was established at Gopalpur, and in 1998 it was rechristened as the Army Air Defence College after the Corps of Army Air Defence became an independent arm of the Indian Army.Training at the college is rigorous and comprehensive.

Courses cover weapon handling, radar and surveillance operations, air defence tactics, leadership development and physical conditioning. Modern simulators and technical training aids complement field exercises, ensuring that personnel are fully prepared for contemporary and future air defence challenges. The college also conducts specialised courses for personnel from other services and friendly foreign countries, enhancing jointness and international cooperation.

The Army Air Defence College stands as a symbol of vigilance, discipline and technological excellence. By producing highly trained air defence warriors, it makes a crucial contribution to India's military readiness and the protection of its airspace.



Invited Dignitaries & Keynoters

Dr Ali Yuce
Professor, Cappadocia University, Turkey

Ali Yuce was born and grew up in Turkey. He altered his life dramatically and profoundly to pursue his passion for academia after working independently for his business. After receiving his Bachelors degree from DePaul University, he obtained his Masters and Doctoral degrees from Eastern Mediterranean University. Before graduating from the Ph.D. program, he worked as an independent researcher concerning tourism and digital technologies and was a part-time instructor at Cappadocia University. Ali Yuce has been teaching at Cappadocia University since 2019, at the undergraduate and graduate levels. He is also associated with "Social and Strategic Studies Centre" and "Tourism Data Processing, Innovation, and Project-Based Research and Application Centre," to implement strategies that will assist in preserving Cappadocia & its distinctive cultural and natural heritage assets.

Dr. Anshuman Roy

Rhombus International

Dr. Anshuman Roy is the Founder and Chief Executive Officer of Rhombus Power Inc., a cutting-edge artificial intelligence company trusted by the United States national security enterprise, including the U.S. Air Force and U.S. Strategic Command. Driven by a passion for solving complex, high-impact problems, Dr. Roy focuses on harnessing artificial intelligence at the intersection of national security, civilian safety, and advanced technology, with a vision to strengthen America's global leadership in AI for the coming century.

Invited Dignitaries & Keynoters

Dr. Balamati Choudhury

Senior Principal Scientist,
CSIRNAL, Bangalore

Dr Balamati Choudhury is working as Senior Principal Scientist at Centre for Electromagnetics of CSIR-National Aerospace Laboratories, Bangalore, India. Her active areas of research and teaching interests are in the domain of: Stealth technologies, Soft Computing Techniques in Electromagnetic Design and Optimization, Computational Electromagnetics for Aerospace Applications, Metamaterial Design Applications, RF and Microwaves. More specifically, the topics of the sponsored projects she has contributed to are development of Ray Tracing Techniques towards RF Analysis of Propagation in an Indoor Environment, Low RCS design, Phased Arrays and Adaptive Arrays, Conformal Antennas. She was recipient of ICCCES/ Outstanding Young Investigator Award for the year 2016-2017 and recipient of the CSIR-NAL Young Scientist Award for the year 2013-2014.

Dr. Binoy K. Das

DG, DRDO Bengaluru

Dr. Binay Kumar Das is a renowned Indian scientist and a senior leader at the Defence Research and Development Organisation (DRDO). He was appointed as the Director of the Instruments Research and Development Establishment (IRDE), Dehradun, becoming the first Odia scientist to head IRDE, one of DRDO’s premier laboratories. IRDE is dedicated to the research, design, development, and technology transfer of optical and electro-optical instrumentation for defence services. Dr. Das began his professional journey in 1987 at the Integrated Test Range (ITR), Chandipur

Invited Dignitaries & Keynoters

Shri G. C. Pati

Former Chief Secretary of Odisha

Shri Gokul Chandra Pati is a senior Indian Administrative Service (IAS) officer of the 1978 batch from the Odisha cadre, with a distinguished career in public administration at both the state and central levels. He is currently serving as the Secretary, Defence Production, Government of India, a key position responsible for strengthening India's defence manufacturing ecosystem and promoting indigenous production.

With decades of administrative experience, Shri Pati has been closely associated with policy formulation and implementation in strategic and governance-related sectors. He is widely regarded as a seasoned administrator known for his leadership and deep understanding of governmental processes.

Major Gen Atanu K. Patnaik (Retd)

Director, Centre for Indology & Culture

Major General Atanu Pattanaik is a decorated Indian Army officer awarded the Sena Medal (Gallantry) & Bar by the President of India. An alumnus of Sainik School Bhubaneswar, he joined the NDA in 1979 and was commissioned into the Regiment of Artillery in 1983. A seasoned helicopter pilot, he has flown extensively in Siachen and along the Indo-China border, and is a graduate of the US Army Aviation Center, Fort Rucker. He has commanded a frontline brigade in Sikkim, served as Chief of Staff of a major Corps, and held the appointment of Addl DG at Army HQ. A PhD in Psychology and prolific writer, he currently serves as Director, Centre for Indology and Culture, Bharatiya Vidya Bhavan, Bhubaneswar.

Invited Dignitaries & Keynoters

Dr Noor Zaman Jhanjhi

Senior Professor, Taylor's University, Malaysia

Prof. Dr Noor Zaman Jhanjhi is a distinguished Senior Professor of Computer Science at Taylor's University, Malaysia, where he specializes in Artificial Intelligence and Cybersecurity. As the Director of the Research Centre, Centre for Intelligent Innovation, and Program Director for Postgraduate Research Degree Programmes, he plays a pivotal role in shaping academic excellence and driving cutting-edge research initiatives. Globally acclaimed for his scholarly contributions, Prof. Jhanjhi has been consistently ranked among the world's top 2% research scientists and stands as one of Malaysia's top computer science researchers. His exceptional work has earned him prestigious accolades, including the Outstanding Faculty Member Award (MDEC Malaysia, 2022).

Dr. Vijay Kumar Sutrakar

Scientist 'F' & Head – Stealth Technologies Division, ADE, DRDO, Bangalore

Dr. Vijay Kumar Sutrakar holds degrees of BE (Mechanical Engineering) from Government Engineering College, Rewa 2002; M. Tech. (Design Engineering), from Indian Institute of Technology, New Delhi, 2004; and PhD (Aerospace Engineering), (Gold Medalist) from Indian Institute of Science, Bangalore, 2013. He joined DRDO in 2004 as Scientist 'B'. Presently, he holds the post of Scientist 'F' and Head – Stealth Technologies Division of ADE and responsible for Design and Development of Low Observable Technologies for India's Prestigious Manned and Unmanned Combat Aerial Vehicle programs. He has more than 22+ years of industry and academic experiences. He has reviewed more than 200+ journal articles for more than 25+ international journals, published 80+ articles in International Journals/Conferences, 3 book chapters, and 200+ Technical articles. He is Fellow of Royal Aeronautical Society, London, UK.

Invited Dignitaries & Keynoters

Dr. Niladri Roy
SC-G, Addl. Director,
ITR Chandipur

Dr. Niladri Roy presently holds the post of Additional Director, Integrated Test Range, DRDO Chandipur. He did his Master in Physics from Ravenshaw College under Utkal University and was the topper of his batch. For some time he worked as a research scholar in BHU, and worked in the field of Nematic liquid crystal display. In 1995, after completion of the DRDO Electronics Fellowship Course at Institute of Armament Technology (IAT), Pune, he joined as scientist in Integrated Test Range. Currently he is heading the Division of Radar, Electro Optics, High speed photography and Meteorology and along with additional charge of Director of Management Services. His research interest includes Radar technology, Data processing, Radar cross section studies, stealth technology, Radome and Radar absorbing materials. He has publications in reputed journals in the field of Ferro and Para Electric materials and their application in Phase Array Antenna and Phase Shifters. He is a member of IEEE and presented papers in international Conferences. His citation includes two times laboratory level group award and twice DRDO National level group award.

Program Agenda

SCHEDULE OF CONDUCT: INTERNATIONAL CONFERENCE ON AIR DEFENCE AND SECURITY 2026 (ICADS-26)

Sl. No	Time	Event	Location
Day 1: 12 Feb 2026 (Thursday)			
1	9:00-1:00 PM	Registration	Atrium Bldg. Lobby
2	10:00 - 11:30 AM	Inaugural Session • Chief Guest: Dr. Binoy Kumar Das, DG, DRDO Bengaluru • Guest of Honor: Shri Gokul Chandra Pati, IAS, Former Chief Secretary, Odisha • Special Guests: Sr Military Officers from Army AD College • Dr. Niladri Roy, SC-G, Addl. Director, ITR Chandipur • Brig. Dr. L C Patnaik (Retd), Indian Army • President, NIST University • Vice Chancellor, NIST University	Stephen Hawking Cineplex
3	11:30 - 12:00 PM	Keynote Speaker 1: Dr. Binoy Kumar Das, DG, DRDO Bengaluru	Stephen Hawking Cineplex
4	12:00 - 12:30 PM	Keynote Speaker 2: Dr. Niladri Roy, SC-G, Addl. Director, ITR Chandipur	
5	12:30 - 1:00 PM	Keynote Speaker 3: Brig. Dr. L C Patnaik (Retd), Indian Army	
6	1:00 - 2:00 PM	Lunch	VVIP: Executive dining room Delegates: Yoga Center
7	2.15 - 4:30 PM	Technical Sessions (Parallel) Session-1- Technological Innovations Session-2: Cyber Security and Defence System Session-3: AI in Defence Session-4: Surveillance & Threat Monitoring	Management Lecture Hall 1 & 2, Galleria Bldg.-310, & Atrium Bldg. 105
8	4:30 - 5:00 PM	Invited Talk : Dr. Noor Zaman Jhanjhi-Senior Professor, Taylor's University, Malaysia	Management Lecture Hall 2
9	4:45 - 5:15 PM	High Tea	Atrium and Galleria Bldg.
10	9:45 - 5:00 PM	Know Your Army Equipment Display + Vendor Exhibition	Atrium Lobby+ Hide Park
11	6:00 - 9:00 PM	Cultural Program & Banquet Dinner	Mayfair, Gopalpur- on-Sea

Sl. No	Time	Event	Remarks/Location
Day 2: 13 Feb 2026 (Fri)			
1	9:30-12:00 PM	Registration	Atrium Bldg. Lobby
2	10:00 - 10:45AM	Opening Session • Chief Guest: Lt Gen RC Srikanth, AVSM, VSM, Commandant, Army AD College • Guest of Honor: Dr Balamati Choudhury, Senior Principal Scientist, CSIR-NAL, Bangalore • President, NIST University • Vice-Chancellor, NIST University	Stephen Hawking Cineplex
3	10:45 - 11:15 AM	High Tea	Atrium & Galleria Bldg.
4	11:15 - 11:45AM	Keynote Speaker 1: Dr. Anshuman Roy, Rhombus Intl (Online)	Stephen Hawking Cineplex
5	11:45 - 12:15PM	Keynote Speaker 2: Dr Balamati Choudhury, Senior Principal Scientist, CSIR-NAL, Bangalore	
6	12:15 - 12:45PM	Keynote Speaker 3: Dr Ali Yuce, Professor, Cappadocia University, Turkey	
7	12:45 - 1:45 PM	Lunch	Executive Dining Room & Yoga Center
8	2:00-4:00PM	Technical Session (Parallel) Session-5: Defence Strategic Environment Session 6: Specialized Defense domains and Future Readiness Session 7: Data driven Security Systems Session 8: Information Warfare	Management Lecture Hall 1 & 2, Galleria Bldg.-310, & Atrium Bldg. 105
9	4:00 - 4:30PM	High Tea	Atrium & Galleria Bldg.
10	10:00 - 6:00 PM	Know Your Army Equipment Display + Vendor Exhibition	Atrium Lobby+ Hyde Park
11	4:30 - 5:00PM	Keynote Address: Dr. Vijay Kumar Sutrakar, FRAeS, FIE, Scientist 'F' & Head – Stealth Technologies Division, ADE, DRDO, Bangalore	Stephen Hawking Cineplex
12	5:00 - 5:45PM	Valedictory Session Conference report: General Chairs Felicitation ceremony: Org Chair, Exhibitors, Sponsors Concluding Remark: Lt Gen RC Srikanth, AVSM, VSM, Commandant, Army AD College Vote of Thanks: Program Chair	Stephen Hawking Cineplex
13	5:45 - 6:30PM	High Tea and Networking	Atrium

Enhancing AI powered Cyber Defence: An Explainable and Resilient Framework for Future Intelligent Warfare

B. Ujalesh Subudhi, Bandhan Panda, Santosh Kumar Kar, Brojo Kishore Mishra*

Department of computer Science & Engineering, NIST University, Berhampur, India
Correspondence: brojomishra@nist.edu

Abstract

Comparing the situation to the current dynamic digital environment, this paper identifies the novel contribution of Artificial Intelligence to the improvement of the contemporary cybersecurity defence mechanism. The paper proposes an innovative AI-enabled defence framework to overcome the pressures of next-generation warfare and the problematic hybrid states. Unlike the conventional approaches that mainly focus on predictive threat recognition and automated recovery when it comes to the topic of cyber security of the enterprise, this research broadens the range of the AI implementation to the national security and tactical defence. The framework combines the notion of cyber resilience, explainable AI (XAI), and autonomous decision-making intelligence in a synergistic way to make the operations more transparent, flexible, and strong. The system provides adaptive threat detection systems and dynamic response systems that can handle both known and a zero day attacks through the integration of deep learning and reinforcement learning. Special resilience layer will guarantee continuity in case of severe disruption, whereas XAI will advance interpretability and accountability so that defense officers can comprehend and rely on AI-based insights. The assessment outcomes have shown a high level of accuracy in response speed, accuracy in the analysis, and fault tolerance when compared to the current models based on AI. This study indicates that adaptive AI architectures ethically managed can transform militant and cyber security defense, making AI one of the primary elements in the defense of resiliency, transparency, and readiness against future challenges.

Keywords:
Artificial Intelligence, Cyber Resilience, Explainable AI, Intelligent Defense, Autonomous Systems, Threat Prediction

AI-driven battlefield decision support using probabilistic threat modeling (Bayesian Networks) integrated with multi-objective optimization (NSGA-II)

Joe Prathap P M 1, Thanushree C Somapur 1, W Vinil Dani 2

1 Department of Computer Science and Engineering Sapthagiri NPS University, Bengaluru India.
2 Department of EEE, Sapthagiri NPS University, Bengaluru, India.
Correspondence: vinildani@snpsu.edu.in

Abstract

Modern battlefield environments are characterized by high uncertainty, dynamic threat evolution, and the need for rapid, data-driven decision-making. Traditional rule-based or deterministic decision-support systems often fail to handle incomplete or ambiguous information, leading to suboptimal mission outcomes. To address this, the present work proposes an AI-driven battlefield decision support framework that integrates probabilistic threat modeling using Bayesian Networks with multi-objective optimization via NSGA-II (Non-dominated Sorting Genetic Algorithm II). The Bayesian Network module estimates real-time threat probabilities by reasoning over uncertain sensor, intelligence, and situational data, providing a probabilistic situational awareness layer. These probabilistic outputs are then used by the NSGA-II optimizer to generate and evaluate tactical decisions based on multiple conflicting objectives—such as maximizing mission success probability, minimizing response time, and reducing resource utilization. The proposed hybrid model is validated through a simulated battlefield scenario using synthetic datasets representing diverse threat conditions and resource constraints. Experimental results demonstrate that the integrated Bayesian–NSGA-II approach yields robust, adaptive, and explainable decision recommendations compared to traditional deterministic systems. This research highlights the potential of combining probabilistic reasoning and evolutionary optimization to enhance real-time decision-making, resource planning, and operational resilience in defense applications.

Keywords:
Battlefield decision support, Bayesian Networks, probabilistic threat modeling, multi-objective optimization, NSGA-II, evolutionary algorithms, AI-driven systems.

Deep Learning Essence in XSS and CSRF

Simar Singh Rayat, Ayush Bhatt, Susheela Dahiya*

Department of Computer Science and Engineering, Graphic Era Hill University,
Dehradun, India
Corresponding: susheela.iitr@gmail.com

Abstract

The advent of advanced computational methodologies has made for a galaxy of operations for users which has precipitated an exponential growth of malicious works like spoofing, poisoning, unsolicited actions, data exfiltration, etc. The present manuscript provides an understanding of Emergent Cyberattacks namely Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF). These attack vectors are constantly evolving and adapting in sync with new technologies such as agentic- based Artificial Intelligence (AI) browsers and adaptive learning browsers. An in-depth review of these cyberattacks is covered in the rest of the paper. The research shows the design and implementation of a proposed framework, which is a multi-layered architecture with Machine Learning (ML) techniques which is designed to analyses, detect, and provide countermeasures to the aforementioned cyberattacks. The framework includes hybrid supervised Deep Learning (DL) models ranging from Temporal Convolutional Neural Networks (CNNs), Graph Neural Networks (GNNs), Variational Autoencoders, and pretrained linguistic models. When combined these models make up a novel methodology for evaluating attack vectors and provide early warning capabilities. The architecture was tested on publicly available datasets such as CSIC 2010, Kaggle XSS datasets, fawaz2015, Malicious and Benign Webpages, etc., which gave an accurate value of 83.21 percent. The model constituents are trained to appraise vulnerability sequence post-preprocessing in order to mitigate noise residuals. Additional essential parts make the framework stand out in its significance and efficacy in real-world deployments. As a result, the framework offers a smart, proactive, dependable, and scalable augmentation to the cybersecurity infrastructure.

Keywords:
Cross site scripting (XSS), Cross site request forgery (CSRF), Deep learning (DL), Convolutional Neural Network (CNN) and Graph Neural Network (GNNs).

A Novel Framework to Convert Public Source URLs to Cryptographic-enabled API Key

Simar Singh Rayat, Sujal Thapa, Susheela Dahiya*

Department of Computer Science and Engineering, Graphic Era Hill University,
Dehradun, India
Correspondence: susheela.iitr@gmail.com

Abstract

The development of digital applications has provided ease in human tasks and diverse capabilities. Industrialists and certain organizations have provided Application Programming Interfaces (abbreviated as APIs). This terminology helps developers in adaptive learning and the development of their tools and applications. APIs are generally a package given by various organizations to authorize private or public users to access specific services; they behave like a two-way medium where the user sends a request and the receiver accepts the request, provides the service, and manages the number of requests. This paper demonstrates the working of an API to understand the proposed framework. Today, digital advancement provides various tools to speed up tasks. Looking at this issue, the proposed framework provides a novel inventive application which allows publicly open-access application Uniform Resource Locators (abbreviated as URL) to be converted into a Cryptographic-enabled API key that works normally like a general public API. The detailed methodology is discussed throughout the paper; many applications provide their API keys that work perfectly and without any obstruction, but during model training, they fetch unrelated data that affects the false positive rate. To address this emerging limitation, our proposed framework allows the user to input a specific URL, which is converted into an API key equipped with a cryptography mechanism to limit data tampering and injection, or other related miscellaneous activities. The proposed framework shows that there has been good advancement in mechanically computing and also offers an adaptive and scalable answer to present-day developer infrastructure.

Keywords:
Application Programming Interfaces (APIs), Uniform Resource Locator (URL), Cryptography, SQL Injection, Private and Public Key.

Analyzing the Impact of LOS and NLOS Propagation on Underwater Localization Accuracy Using Data Collected by Autonomous Underwater Vehicles (AUVs)

Ashish Kumar Dass 1, Sudhir Ranjan Pattanaik 2, Manjushree Nayak 3

1,2 NIST University, Palur Hills, Berhampur, Odisha
3 Amity University, Raipur, Chhatishgarh
Correspondence: manjushreesai44@gmail.com

Abstract

The underwater localization technique is indispensable for marine operations like exploration, habitat monitoring, and search-and-rescue. The acoustic propagation path mainly determines the accuracy of localization methods that may either be line-of-sight (LOS) or non-line-of-sight (NLOS) based. Acoustic propagation through LOS gives a direct path; NLOS, on the other hand, involves a combination of reflection, refraction, and scattering which can either be caused by the seabed, surface, or obstacles. The integration of different methods for underwater localization via AUVs has been evaluated in this review. Considering the existing literature, theoretical models, and experimental observations, the paper sheds lights on NLOS's considerable range bias and position estimation decay. Several techniques such as NLOS detection, bias compensation, sensor fusion, and geometry-aware methods are reviewed under the topic of mitigation approaches. Accompanying simulation and experimental results demonstrate that neglecting NLOS effects can lead to an increase in localization error of more than 40%, while adaptive modeling and data fusion can effectively lessen the impact considerably. The review points out the present research gaps and suggests future directions for AUV-based underwater localization in scenarios with mixed LOS/NLOS conditions.

Keywords:
Underwater localization, Autonomous Underwater Vehicle (AUV), acoustic propagation, LOS, NLOS, TDOA, multipath, sensor fusion.

Practical Implementation of Dubins Method for Path Planning of Fixed-wing UAV using Genetic Algorithm

1,2 Milan Kumar Pal, 1 Minati Mishra, 2 Rajib Kumar Das

1 PG Dept. of Computer Science, FM University Balasore, India
2 ITR, Chandipur, DRDO, India
Correspondence: rajibkudas@gmail.com

Abstract

Unmanned Aerial Vehicles (UAV) or Re motely Piloted Aircraft (RPA) are finding rapidly
increasing applications in various fields. Now a days They are being used for almost each and every role including military Intelligence, Surveillance & Re connaissance (ISR), agriculture, meteorology, disaster management, aerial photography etc. The central idea about the autonomous operation of UAVs is Path Planning. The path to be followed by UAV depends on the type of the UAV, nature of task to be performed, environmental factors and operational space making UAV path planning a multi-objective problem which can be dealt well by meta-heuristic methods like Genetic Algorithm. As Fixed wing UAV kinematics is different from Rotor-craft UAVs, separate approach is required to be adopted for path planning to suite the non-holonomic nature of the flight. In this paper, A genetic Algorithm based path planner has been implemented in python using simplified Dubins path method to generate flight path of a fixed wing UAV
in a constrained environment .

Key words:
Path Planning, Dubins Path, Genetic Algorithm, Adaptive Speed Contro

Rotation-Dependent RCS Signature Analysis and Machine-Learning-Based Identification of a Chipless RFID Tag for Passive Defence Sensing Applications

Rashmirekha Kalyani Mishra, Santanu Kumar Behera, Rabindra Kishore Mishra

Department of ECE, NIT, Rourkela, India
Correspondence: prof.r.k.mishra@gmail.com

Abstract

Defence, logistics and security services are using low-cost and passive Chipless Radio Frequency Identification (CRFID) technology for identification applications. Rotation-dependent spectral variation degrades tag readability when using bistatic radar-style interrogation due to polarization mismatch which reduces the measurable Radar Cross Section (RCS). In this work the possibility of employing AI to negate such effect is the centre of investigation when analyzing backscattered spectral signature of frequency-coded CRFID tag. It employs a compact CRFID tag on 1.6mm thick FR4 substrate (7cm x 7cm) containing 18 corner slotted concentric square-ring resonators. The tag characterisation uses EM simulations of RCS (for rotation angles of 0°, 15°, 30°, and 45°) and laboratory bistatic measurement (for 0°) on fabricated prototype. Baseline correction via median filtering gave equivalent RCS of measured for comparison with simulation results. Application of controlled frequency warping, noise injection, and amplitude scaling generated synthetic experimental dataset from four simulated orientations expanding them to 800 unique signatures. These spectral traces trained and evaluated two machine-learning (ML) pipelines: a dip-feature Support Vector Machine (SVM) classifier and a 1D Convolutional Neural Network (CNN). The accuracy in the former is between 72–75% while in the later it is around 80%. Results show possibility of high accuracy orientation classification through data-driven methods confirming availability of sufficient encoded information within the rotation-induced spectral variation. So, in future passive defence and security systems can employ AI (ML-assistance) for identification and authentication.

Keywords:
CRFID, RCS, Rotation Classification, ML, CNN, SVM

Adversarial Robustness in LLMs: A Survey of Attacks and Defences with Experimental Evaluation of Decision-Based Attack and Human-in-Pipeline Defence

Prachi Subhadarsini Sahoo, Minati Mishra

Fakir Mohan University, Balasore, Odisha, India
Correspondence: minatiminu@gmail.com

Abstract

Natural Language Processing (NLP) has witnessed remarkable progress with the advent of Large Language Mod- els(LLMs) such as GPT, Gemini, Claude, and LLaMA, which demonstrate powerful capabilities in text generation, reasoning, and human like response. However, their susceptibility to ad- versarial manipulation poses a significant threat, particularly in defense and security sensitive applications where reliability and robustness are paramount. Even subtle perturbations or carefully crafted prompts can mislead LLMs into producing harmful or misleading content, undermining mission critical systems.

This paper presents a study on adversarial attacks and corresponding defense strategies for LLMs, emphasizing upon the decision based black box attack and the Human-in-Pipeline (HIP) defense paradigm. Through comprehensive analysis, it is observed that while existing countermeasures are promising, they remain fragmented, context dependent, and lack scalability for deployment in real world defense systems. The findings prove that there is a need for integrated, adaptive, and explainable defense mechanisms to ensure secure and trustworthy LLM utilization in defense intelligence, cyber operations, and decision support environments.

Keywords:
Adversarial Attack, Large Language Models, Cybersecurity, Defense Mechanisms, Robust AI systems.

Adversarial Robustness and Explainability in Intrusion Detection Systems: Maintaining XAI Integrity Under Adversarial Attacks

Parthiv Gopa, T Grace Shalini

Department of Computational Intelligence, SRM Institute of Science and Technology, Chennai, India
Correspondence: gopaparthiv@gmail.com

Abstract

Military networks are susceptible to cyber attacks. Intrusion Detection Systems (IDSs) are developing to defend military assets using machine learning models combined with explainable techniques, such as SHAP, allowing military operators to have high accuracy when detecting intrusions, yet also be able to understand how decisions are made. However, there still remains the critical area of researching the interactions between adversarial attacks and explainability for IDSs. This paper tries to fill this gap by looking into the interactions between adversarial attacks and explainable AI (XAI) in terms of network intrusion detection. Our research demonstrates that existing IDS models have moderate accuracy (70.6% classifying a FGSM attack, and 70.8% classifying a PGD attack), however, the SHAP explanations for the model become less accurate during adversarial attacks. Therefore, the operators may not trust the accuracy of the IDS model's output due to less accurate model explanations. We propose an adversarial training method that improves the overall robustness of the model (80.6% classifying a FGSM attack, and 80.4% classifying a PGD attack) while maintaining reliable SHAP explanations. Additionally, our results indicate that XAI explanation stability can be preserved during adversarial training, which creates an opportunity to close a major research gap in the fields of robustness and interpretability. Thus, this study will enable military operators to be confident in making AI-driven support decisions during military operations where military operations require both high accuracy and high transparency in their decision-making.

Keywords:
Intrusion Detection Systems, Adversarial Ro bustness, Explainable AI, SHAP, Machine Learning Security, Defense Systems, Network Security

Post-Quantum Cryptography using CRYSTALS-Dilithium on Application of Defense Security Systems

Apurva Singh 1, Sudipta Sundar Biswal 1, Bibhuprasad Mohanty 1, Mihir Narayan Mohanty 2*

1 Electronics and Communication Engg., Siksha O Anusandhan University, Bhubaneswar, India
2 Faculty of Engineering and Technology, Siksha O Anusandhan University, Bhubaneswar, India

Correspondence: mihirmohanty@soa.ac.in

Abstract

To break traditional cryptographic systems with algorithms like RSA and ECC, Quantum computing is an alternative for defense communications and data security. Post-quantum cryptography (PQC) offers quantum-resistant algorithms to secure sensitive defense infrastructures against potential quantum attacks. This paper discusses the post-quantum security algorithms, named as the CRYSTALS-Dilithium digital signature scheme, in order to improve the security infrastructure of defense systems from future quantum computing threats. The work explores the design principles, implementation challenges, simulation methodology, and performance evaluation suitable for defense applications. It demonstrates that the PQC algorithms are the future-proof defense communication, authentication, and data integrity. It is NIST-standardized post-quantum digital-signature scheme based on lattice assumptions, and it provides one viable pathway to safeguard current and future defense systems.

Keywords:
Post Quantum Cryptography, CRYSTALS-Dilithium, Defence Security, Quantum-Resistant Signatures, Cybersecurity, Cryptographic Agility

Implementation of Securing Text Data Using Steganography and Cryptographic Techniques

Sukhhma Shetty, Sowmya K, Shreejith D Shetty, Sunil, Vinay Poojari S, Deepak Shenoy

Department of Computer Science and Engineering, Canara Engineering College, Mangaluru, India
Correspondense:deepakshenoy119@gmail.com

Abstract

Contemporary conditions call for an effective means of protecting sensitive text information from being intercepted and subsequently analyzed due to the increasingly heavy use of digital communications. Primarily, the efficiency of traditional approaches that implement only one security mechanism of encryption or steganographic embedding often becomes poor under modern network surveillance tools and steganalysis soft ware and techniques. This article proposes the concept of the two-layer security scheme utilizing AES-256 encryption, SHA- 256 for generating the key, and the Bi-LSB image embedding method. In the first layer of security, the provided passphrase is hashed to produce a 256-bit key via the SHA-256 hashing function, coupled with AES-256 encryption of the text that would render it unreadable even if intercepted by an intruder. Afterwards, an encrypted data output is subsequently hidden inside an image file by employing the concept of mindless two bit LSB replacement, thus ensuring that the image is remaining untouched with no apparent changes.A prototype is developed with the objective of verifying the efficiency of the encryption and key procedures and image quality. It was found that due to distinct initialization vectors, there is always a different output from all encryption routines with the; hence, it limits the risk for pattern-based attacks. Incorrect keys, modified ciphertext, and malformed input data have been consistently rejected by the system; integrity safeguards are very strong. The Bi-LSB method also maintained the visual quality of the carrier images while secretly concealing the encrypted text. Security analysis indicated protection levels of about 95% for AES-256, 90% for bcrypt, 85% for SHA-256, and 80% for Bi-LSB can be attained. In general, the combined framework provides a practical and covert approach for transmitting sensitive text in environments where confidentiality and invisibility are critical.

Keywords:
Cryptography, Steganography, AES-256, SHA-256, Bi-LSB, Secure Communication

Xeno Cipher: A Secure Key Exchange and Encryption Pipeline for Resource-Constrained Devices

Alok Ranjan, Vivek S A, Subramanyam C V, Sujal Talekar, Sumit S Kadwadkar

Department of Computer Science and Engineering, Canara Engineering College, Mangaluru, India
Correspondence: kadwadkarsumit333@gmail.com

Abstract

In the current modern world due to the rise of Internet of Things there is an increase in the use of connected devices, these devices such as smartwatches, smart thermometer constantly sense and collect telemetry data from their environment and may send the collected data to a remote server located in the cloud for analytical processing. The data being sent has to be protected using an suitable cryptographic encryption/decryption system. However the challenges faced in the current systems are; traditional encryption algorithms like AES, RSA, ECC are not suitable for encrypting data in these devices because the devices have limited computational resources and these algorithms were designed for powerful systems such as pc, laptop, smartphones etc, current literature mainly focusses on fixed mode encryption, there is no runtime adaptability introduced in generating ciphers, most of the lightweight ciphers and have single layered and static pipeline which is vulnerable to cyber attacks. Therefore in our quest to find solutions for these problems Xenocipher was developed. Xenocipher is a secure, lightweight, multilayered cryptographic system that operates at bit/stream level. It combines three lightweight symmetric algorithms in a layered fashion to generate strong ciphers, they are LFSR(Linear Feedback shift register) for pseudorandom stream generation, Chaotic map for entropy and non linearity and bit level transposition for diffusion. Along with this core pipeline the system also provides an adaptive switching feature called ”Zero Trust Mode” which aids in detecting threat pattern and dynamically switches to one of the five encryption recipes based on the live heuristic feedback. To exchange the master key generated at the device with a server a post quantum asymmetric key is used called NTRU. It generates the key pair at the server and shares it with the device, the device encrypts the master key and transmits it to the server over the network, the server decrypts it and obtains the master key. The system was tested using an ESP32 microcontroller and a C++ server. It achieved a median encryption time of 52.5 ms for every 106 byte packet. The ram used during the encryption process was 12KB out of 512KB. The entire module occupied 180KB of the flash and around 22% of the cpu load.

Keywords:
AES, RSA, ECC, NTRU

LLM-Based Agentic Decision Support for Maritime Threat Assessment

Krishikaa Mathi Bharathi S S, T. Grace Shalini, Bhavesh P, Nayantra Ramakrishnan

Dept of Computational Intelligence, SRM Institute of Science and Technology,
SRM University
Correspondence: graceshaliniphd@gmail.com

Abstract

Maritime border security remains a significant chal- lenge, particularly due to the low false-positive requirements of detection systems, unreliable AIS data, and the scarcity of labeled datasets needed for conventional deep learning models. To address these constraints, this work proposes a software-only, multi-agent decision-support framework that integrates unsuper- vised trajectory anomaly detection with large language model (LLM)-based threat reasoning for real-time maritime situational awareness. The system employs a self-supervised Variational Au- toencoder (VAE) trained on publicly available AIS datasets to de- tect deviations in vessel behavior without domain-specific labels. An LLM-based analytical agent then interprets these anomalies within an operational context. Additionally, a decentralized multi- agent coordination protocol enables distributed situational assess- ment across multiple maritime zones. By allowing independent agents to jointly evaluate risk indicators, exchange high-level signals, and generate clear, human-understandable explanations, the framework enhances robustness, reduces false alarms, and strengthens human-machine teaming. Early evaluations on real- world AIS pathways indicate promising performance with high anomaly-detection accuracy, low response time, and efficient multi-agent coordination. Overall, this study presents a prac- tical, explainable, software-centric strategy to improve maritime border surveillance, demonstrating how agentic, LLM-powered intelligence can enhance national defense processes in dynamic and information-poor environments.

Keywords:
Autonomous Vessel Detection, Maritime Surveil- lance, Large Language Models (LLMs), Multi-Agent Systems, Variational Autoencoder (VAE), AIS Data, Anomaly Detection, Threat Characterization, Human–Machine Teaming, Maritime Domain Awareness, Defense Decision Support Systems, AI Sys- tems.

Smart Autonomous Surveillance Rover (SASR)

Sneha, Madan Lal Sain

Department of AIML (AIT-CSE), Chandigarh University, Mohali, Punjab, India
Correspondence: mlsaini@gmail.com

Abstract

Real-time surveillance is critical for protecting sensitive and dynamic environments, but static systems like CCTV have inherent limitations like fixed coverage and vulnerability to tampering. In this paper, we propose a Smart Autonomous Surveillance Rover, integrating Raspberry Pi for computation and networking and Arduino UNO for real-time hardware control. It provides autonomous navigation with camera-based obstacle detection and an A* algorithm for optimal path planning, real-time video streaming over a web interface, dual-mode remote/autonomous control, and voice command support. It delivers scalable, secure, and interactive surveillance for homes, industrial sites, and public areas. An accuracy of 87.59% in obstacle avoidance rate demonstrates precise navigation and other parameters like robust real-time streaming, flexible operator interface, and low latency enable effective use in security-sensitive domains.

Keywords:
Autonomous Surveillance Rover, Raspberry Pi, A* Algorithm, Real-Time Video Streaming, Voice Command Control

EdgeWise Pretrain: Few-Shot Graph Intrusion Detection for Heterogeneous Networks

Irfan Mohd

Deccan College of Engineering & Technology, Hyderabad, India
Correspondence: mdirfan61975@gmail.com

Abstract

Maintaining modern computer systems, networks contains detectors that have a method of stopping unwanted external users on system. This article is written about a new paper that presents a new sort of highly accurate method for identifying network intrusions without the need for any additional hardware. The proposed method is a way to model which hosts and protocols behave together in order to identify coordinated behaviors on the lowest level, while excluding this being because of hosts or something. That pretraining pipeline maintains a good overall efficiency by scoring an impressive 95 percent on a wide variety of benchmarks and only requires under 4 percent of the original data. The outcomes of this method show that active training methods lead to accurate network protection no matter the situation.

Key words:

Graph Neural Networks, Self-Supervised Learning, Network Intrusion Detection, Dense Feature Embedding, Cybersecurity, Representation Learning.

Spectral Attention GNN Framework for Secure Telemetry in UAV and Satellite Communication Systems

Yogendra Chhetri

Department of Centre for Continuing Education, Indian Institute of Science, India
Correspondence: chhetri.com@gmail.com

Abstract

Observed the rapid rise of Unmanned Aerial Vehicles (UAVs) in the past decade as well as the emergence of several satellite enabled systems, which have introduced new cybersecurity vulnerabilities associated with their predictable behavior, broadcast communication, and limited onboard processing capabilities. Traditional IDSs have deficiencies in real-time high-speed telemetry analysis and later correlation of zero-day attacks [8]. In this paper we introduce a new hybrid intrusion detection framework, leveraging a spectral attention graph neural network (SA-GNN) and XGBoost to combine topological information and gradient-based classification to overcome these obstacles. The SA-GNN model boosts the node embeddings with spectral scores based on Laplacian eigencomponents, thus effectively encoding global graph structures which show network anomalies. These representations are then passed into an XGBoost classifier for decision.The UAVIDS-2025 dataset experiments demonstrate noticeable enhancements on top of the state-of-the-art methods. Compared SVM-based models resulted in a maximum of 96.08% accuracy, 90.6% F1-score, and 91.47% precision, indicating that our model is better than Deep MLP Ensembles, LSTM-Attention, and the SVM-based. The impact of spectral attention & graph-based modelling briefly, ablation studies also validate the necessity of those techniques — spectral attention (+2.5% accuracy gain) & graph (+4.8% AUC-ROC improvement). This architecture exhibits significant detection robustness over a wide range of intrusion types, including Sybil, Flooding and Wormhole attacks, establishing its feasibility for mission-critical applications based on UAVs.

Keywords:
UAVIDS-2025, SA-GNN, XGBoost, Spectral Attention, UAV Intrusion Detection, Graph Neural Network, Anomaly Detection, Cybersecurity, Telemetry Analysis.

Hybrid Orthogonal CNN–ResNet50 with Grey Wolf Optimization for Malware Classification on MalNet

1 Yogendra Chhetri, 2 Deepika, 3 Sukhvir Kaur

1 Department of Centre for Continuing Education Indian Institute of Science, India
2 School of Engineering and Technology (SET), CGC University, Punjab, India
3 Department of Computer Science and Engineering, Chandigarh University, Punjab, India
Correspondence: deepikalibra@gmail.com

Abstract

The rapid increase in the number of different forms of malware has made it difficult to rely on signature-based detection methods. The main contribution of this paper is a new hybrid model whereby the OCNN and ResNet50 are used in combination, optimised using GWO for feature weighting selection, and the classification is based on ensemble learning techniques. Our approach is tested on the MalNet image-based malware dataset, achieving better results than state-of-the-art methods. The proposed architecture obtains 99.2% for accuracy and robust class-wise studying performance. Based on extensive 5-fold cross-validation, in addition to comparison with previous research, we analytically verify the efficiency of our hybrid architecture for the detection & classification of malware families from visual presentations.

Keywords:
Malware Detection, Orthogonal CNN, ResNet50, Grey Wolves Optimization, Ensemble Learning, MalNet Dataset, Deep Learning

Privacy-Preserving Collaborative Threat Intelligence for Predictive Cyber Defense

Guru Prasad Reddy K, R. Saranya, Santhi M, Rajendran Thanikachalam, Satheesh Kumar.M, B. Aishwarya

Computer Science and Engineering (Cyber Security), Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India.
Correspondence: aishwaryabakthavachalan@gmail.com

Abstract

The rapid increase in coordinated cyberattacks has exposed the limitations of isolated security monitoring. Although collaborative threat intelligence can enable earlier detection of distributed campaigns, privacy regulations, trust barriers, and governance requirements often prevent organizations from sharing raw security telemetry. Existing approaches, including standardized sharing frameworks, anonymization techniques, federated learning, and homomorphic encryption prototypes, address parts of this challenge but suffer from high overhead, limited analytical value, or lack of integrated governance. This work presents a collaborative threat intelligence platform that enables cross-organization analysis without exposing raw telemetry by combining Fully Homomorphic Encryption (FHE), tokenized equality matching, Differential Privacy (DP), and permissioned blockchain-based auditing. The platform further integrates deception-based telemetry and predictive analytics operating on privacy-preserving features to support early detection of coordinated attacks. Experimental evaluation under multi-tenant workloads demonstrates approximately 2.1 hours of earlier detection compared to isolated plaintext analysis, while maintaining acceptable accuracy under differential privacy constraints. These results indicate that predictive, privacypreserving, and auditable collaborative threat intelligence is feasible for deployment in regulated environments.

Key Words:
Homomorphic Encryption, Differential Privacy, Threat Intelligence, Privacy-Preserving Analytics, Predictive Defense, Secure Multi-Party Computation, Honeypot Telemetry.

Quantum-Enhanced Blockchain for Optimized Supply Chain Management: Leveraging QAOA and Secure Transaction Protocols

L Sherin Beevi 1, Ponsy R K Sathia Bhama 2, Joe Prathap P M 3, Muthupandian V 3

1 Department of Computer Science and Engineering, R.M.D. Engineering College, Kavaraipettai, INDIA.
2 Department of Computer Technology, Madras Institute of Technology, Anna University, Chromepet.
3 Department of Computer Science and Engineering, Sapthagiri NPS University, Bengaloru.
Correspondence: muthupandianv@snpsu.edu.in

Abstract

A quantum-enabled blockchain architecture for secure and efficient supply chain management is created by combining quantum optimization, decentralized transaction control, and post-quantum security enforcement. Supply chain decision factors such as supplier allocation, routing optimization, and inventory coordination are framed as combinatorial optimization problems and solved using the Quantum Approximate Optimization Algorithm. The optimum decision outputs are carried out via blockchain-based smart contracts, which enable automatic validation, transparent processing, and immutable transaction storage. A quantum-resistant security layer allows for safe authentication, encrypted communication, and attack-resistant transaction verification against both classical and quantum adversaries. A multi-tier simulated supply chain environment is used to evaluate system performance, which includes measures such as latency, throughput, optimization accuracy, security resilience, and operational cost. When compared to traditional supply chain and blockchain-based implementations, the results show faster convergence, lower transaction latency, more security, and greater transparency. The findings support the efficacy of combining quantum optimization, decentralized ledgers, and quantum-resilient encryption for next-generation intelligent supply chains.

Keywords:
QAOA, Smart contract Data, Quantum Optimization Layer, Quantum Resistant Protocol.

Smart Cybersecurity: A Dataset-Driven Comparative Analysis of ML Techniques for Network Intrusion Detection and Prevention

Astha Das 1, Saurabh Bilgaiyan 2, Anuradha Vashishtha 3, Amartya Chakroborty 1

1 Computer Science & Communication Engineering, KIIT-Deemed to be University, Bhubaneswar, Odisha, India
2 School of Computer Engineering, KIIT-Deemed to be University, Bhubaneswar, Odisha, India
3 Computer Science & Engineering, Khalsa College of Engineering & Technology, Amritsar, Punjab, India
Correspondence: 2329171@kiit.ac.in

Abstract

A Network Intrusion Detection System (NIDS) plays a crucial role in cybersecurity protection. We can observe that cyberattacks have a complex structure, with the primary goal of targeting global networks. Traditional signature-based detection techniques are unable to identify emerging threats such as zero day exploits. This study uses machine learning classifiers such as LightGBM, CatBoost, and XGBoost. To train these models, we use the most effective datasets for network intrusion detection, which are UNSW-NB15 and NSL-KDD. These are useful for both normal and malicious network activities. However, the challenges we encountered include imbalanced data, computational efficiency, and feature selection. This study provides the performance of XGBoost, LightGBM, and CatBoost classifiers, which analyze the trade-offs between their ROC curves and Precision-Recall curves to better understand their performance, especially on imbalanced intrusion datasets.

Key words:
Machine Learning (ML), Cybersecurity (CS), Intrusion Detection System (IDS), Threat Detection (TD), Network Security

NeuroMesh Sentinel: Decentralized Swarm Intelligence for Autonomous Multi-Cloud Security

Krishnaveni K, Jeevitha K, J.T Anita Rose

Computer Science and Engineering, St. Joseph's College of Engineering, OMR,
Chennai – 600119
Correspondence: anitarosejt@stjosephs.ac.in

Abstract

The Multi-cloud strategies are being embraced by cloud infrastructures, yet centralized security systems pose a single point of failure thus creating lagging breach detection, lateral movement, and log tampering vulnerabilities. This paper presents NeuroMesh Sentinel, a decentralized security architecture that generates cloud resources into autonomous agents and creates a self-organizing mesh network. The system integrates indications of the biological immune system mimicry, swarm intelligence, stigmergic communication, hyperdimensional computing, and Byzantine fundamental fault-tolerant consensus to obtain quick, adaptive discover and reaction to threats. The agents constantly acquire identifying behavioral baselines, identify anomalies, authenticate threats collectively, and automatically apply countermeasures, and blockchain provides cryptographically unalterable audit trails. Prototyping The prototyping phase in the design of this system proved sub-second detection, significant level of false positive reduction, autonomous threat neutralization and resistance to compromised nodes. Also, through the framework, there is also sharing of federated their threat intelligence between organizations without compromising on privacy. NeuroMesh Sentinel is a radical innovation in the field of multi-cloud security providing a scalable, self-evolving and demonstrably resilient architecture that can overcome some of the most inherent disadvantages of the traditional centralized monitoring system.

Keywords:
Multi-Cloud Security, Swarm Intelligence, Distributed Consensus, Autonomous Agents, Blockchain, Behavioral Biometrics, Hyperdimensional Computing.

Hybridization of Meta-Heuristic based Optimization Techniques with RNN- based Machine Learning for Detection of Cyberattacks

Sasmita Panigrahi, Manas Ranjan Patra, Ashalata Panigrahi

Department of Computer Science and Engineering, NIST University,
Berhampur, India
Correspondence: ashalata.panigrahi@nist.edu

Abstract

Network infrastructures play a vital role in today's defense systems. Protecting such networks from cyberattacks is becoming a growing concern. Building Intrusion detection systems (IDS) to protect against sophisticated adversarial cyberattacks is one of the possible solutions in this direction. IDS systems can continuously monitor network activities to identify potential attacks such as Denial of Service (DoS), Probes, User to Root (U2R), Remote to Local (R2L), and Port scan. In this work, an RNN-based model has been developed to detect anomalous behavior of network users. The model employs two meta-heuristic methods namely, Whale Optimization and Gray Wolf Optimization (GWO) for feature selection followed by SMOTE (Synthetic minority oversampling) for class balancing. Next, two classification techniques namely, Simple recurrent neural network (SRNN) and Long Short-Term Memory (LSTM) have been applied for binary and multi-class classification. The proposed model achieves encouraging performance compared to earlier works with an accuracy of 0.9941, lowest FAR of 0.0008 and improvement in other standard performance parameters.

Keywords:
Recurrent neural network, Long Short-Term Memory, Whale Optimization, Gray Wolf Optimization, Synthetic minority oversampling.

A Dual-Model NIDS Architecture Combining Convolutional Neural Networks and Autoencoders for Robust Attack Detection

Robin Jose R, Surya R, Ahila Devi.E

Department Of CSE, St. Joseph's College of Engineering Chennai, India
Correspondence: ahila.me@gmail.com

Abstract

Network Intrusion Detection Systems (NIDS) must accurately identify changing cyber-attacks, including zero-day threats that differ from known patterns. This paper proposes a dual-model NIDS architecture that combines a Convolutional Neural Network (CNN) with an Autoencoder to achieve strong and flexible attack detection. The CNN component performs supervised classification to capture spatial dependencies in net-work traffic features. This enables precise detection of known attack classes. At the same time, the Autoencoder learns compact representations of normal traffic and flags anomalies based on reconstruction errors. This approach helps to detect unseen and zero-day attacks effectively. The outputs of both models are com-bined to create a hybrid decision layer that improves reliability and lowers false positives. Experiments on standard intrusion datasets show that this architecture consistently outperforms traditional single-model NIDS in accuracy, recall, and zero-day detection capability. This dual-model design provides a scalable and reliable framework for modern intrusion detection in today's network environments.

Keywords:
Intrusion Detection System (IDS), Deep Learning, Convolutional Neural Networks (CNN), Autoencoders, Hybrid Model, Network Traffic Analysis.

Geospatial Crime Type Prediction Using Machine Learning

Ms. S.Banumathi, K.Prasanna Anjaneyulu, K.Chandra Sekhar

Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology Chennai, India
Correspondence: vtu22156@veltech.edu.in

Abstract

The rapid growth of crime in urban and semi- urban regions has raised the demand for intelligent systems capable of predicting crime patterns using spatial and temporal data. Geospatial crime prediction is based on historical records of crimes committed and contextual geographic information to anticipate the type and location of future incidents. This paper presents a machine Learning-based approach to predict crime types using geospatial and socio-demographic datasets that provide an analytical framework for proactive policing, such as Random Forest, Support Vector Machine, and Decision Tree, and K-Nearest Neighbors (KNN) are applied to capture the relationship between spatial coordinates, time, and historical crime occurrences. The model predicts not only the likelihood-of crime occurrence but also the type of crime most probable in a given region. Experimental evaluation shows that Random Forest and SVM outperform other models in terms of classification. classification-accuracy, robustness, and generalization. The proposed system demonstrates its potential as a decision- support tool for It helps ensure efficiency in patrol deployment by law enforcement agencies. resource management, and enhanced community safety initiatives.

Index Terms:

Geospatial analysis,MachineLearning,Crime prediction, RandomForest, GIS, Spatial-temporal modeling

Design of an IDS for Detection of Adversarial Attacks in IoT using Machine Learning

Sachit Kumar Nayak, Ashalata Panigrahi

Department of Computer Science and Engineering, NIST University, Berhampur, India
Correspondence: ashalata.panigrahi@nist.edu

Abstract

As the Internet of Things (IoT) expands, the security of IoT networks has becoming more challenging. To address the security issues faced by the IoT network this work proposes metaheuristic optimization techniques namely, Elephant herding optimization (EHO) and Sequential Hybrid of Elephant Herding Optimization and Simulated Annealing (EHO+SA) to select an optimal subset of features that maximize a specific objective function. We use oversampling technique to avoid over-fitting and under-fitting issues that results in biased classification. Two classification techniques namely, deep forest (DF) and deep neural network (DNN) have been implemented for multiclass and binary classification. For evaluation of the model CIC-IoT 2023 dataset is used. The proposed approach reports Oversampling + EHO + DF + Brute-force attack achieves highest accuracy of 0.9999, precision of 1.0, and F-value of 0.9997 and lowest FAR of 0.0. Oversampling + EHO+SA + DF + DoS reports highest recall of 1.0. Oversampling + EHO + SA + DF + DoS reported highest NPV of 1.0 and lowest FNR of 0.0. For binary classification oversampling + EHO+ Deep Forest reports highest accuracy of 0.9944, recall of o.9962, precision of 0.9977, specificity of 0.9672, F-value of 0.9969, and lowest FAR of 0.0328.

Keywords:
Deep Forest, oversampling, Elephant herding optimization, simulated annealing, confusion matrix.

ML and Cloud-Based Turbulence Prediction Model for Aviation Safety

Ananya Karn, Brijmohan Lal Sahu

School of Computer Science, UPES, Dehradun, India
Correspondence: brijmohan.sahu@ddn.upes.ac.in

Abstract

Turbulence is a leading unpredictable hazard in aviation and often remains undetected until an aircraft is already experiencing destabilizing atmospheric conditions. Traditional sources such as onboard weather radar, Pilot Reports (PIREPs), and Air Traffic Control (ATC) advisories are largely reactive and are less effective against Clear-Air Turbulence (CAT). This problem is addressed using a Machine Learning (ML)-based turbulence severity classifier with a Random Forest (RF) algorithm to predict three operationally relevant levels: Low, Moderate, and Severe. The trained model is integrated into an Amazon Web Services (AWS)-based inference service using an Amazon Elastic Compute Cloud (EC2)-hosted Docker container with model artifacts stored in S3. The designed system supports real-time API-based inference, and a browser interface demonstrates operational usage. Full real time ingestion and automated alerting pipelines are outlined as future work. The results suggest practical potential for improving passenger safety and airline operations. Unlike prior turbulence-prediction studies that remain offline, this work includes a cloud-deployable prototype using Docker and AWS, demonstrating a practical pathway toward operational real time turbulence alerts.

Key Words:
Turbulence prediction, MOSDAC L2B, AWS EC2, Machine Learning, Aviation safety

Variance-Guided Adaptive DWT–DCT Image Steganography for Defense and UAV Applications

Gatram Sravan Kumar 1, Mitu Baral 2, Mettu Bhavya Nayana Reddy 3,
Kamalakanta Sethi 4, and G Rama Mohan Babu 3

1 Indian Institute of Information Technology, Sri City, India
2 NIST University, Berhampur, India
3 RVR & JC College of Engineering
4 Indian Institute of Information Technology, Sri City, India
Correspondence: rmbgatram@gmail.com

Abstract

The secure and secret transmission of visual data is a very important need in recent military and monitoring systems, especially when it comes to the use of UAVs and scouting devices. Steganography of images is a technique that is quite efficient in hiding classified data inside common pictures and thus avoiding the detection of illicit communication. A method based on adaptive transform-domain image steganography is introduced herein for defense-oriented applications. DWT and DCT are used in combination to apply embedding with high frequency wavelet sub-bands and secret surveillance images are embedded into mid-frequency DCT coefficients to achieve a good balance between invisibility, robustness, and embedding efficiency. The method achieved the best results in the above aspects through the use of variance-guided adaptive payload that allowed the evolving of embedding strength according to local image texture characteristics. The extensive testing of the new method against its predecessors in terms of Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index Measure (SSIM), and resistance to common image processing attacks which done on standard benchmark images and UAV surveillance data has proven that the new approach indeed performs better than conventional spatial-domain, transform domain, and hybrid steganography techniques. The findings validate the proposed system's capability to facilitate secure and hidden image transmission in military and surveillance operations.

Keywords:
Defense Surveillance, UAV Imagery, Discrete Wavelet Transform, Discrete Cosine Transform, Adaptive Payload Allocation.

Sensitive Data Masking and Security Validation in File Upload System

Edwin Santhosh L 1, Karthick S.A 1, J Sarojini Premalatha 2

1 CSE with Cyber Security Sathyabama Institute of Science and Technology, Chennai, India
2 Dept. of CSE, Sathyabama Institute of Science and Technology Chennai, India
Correspondence: sarojinipremalatha.j.cse@sathyabama.ac.in

Abstract

The widespread use of third-party platforms for document uploads has intensified concerns about data privacy and the unauthorized use of sensitive information. In this work, we develop and evaluate a unified framework for identifying, masking, and validating sensitive content both before and after file upload. The system uses Optical Character Recognition (OCR), natural language processing (NLP), and pattern-based analysis to detect private information such as identification numbers, contact details, and addresses. In the implemented system, a privacy risk score is generated for each document, and high-risk cases trigger dynamic masking or redaction prior to upload. To ensure continued protection, a post-upload validation module monitors third-party handling to detect misuse, unauthorized access, or data leakage. The prototype includes a lightweight, client-side interface that enables secure document submission, real-time analysis, risk reporting, and safe download of sanitized files. The framework is designed to support compliance with global and regional privacy regulations, including the GDPR, Indian IT Act, and DPDP Bill. By integrating automated audit logging and transparency mechanisms, the system delivers end-to-end privacy control and enhances user trust throughout the document upload lifecycle.

Keywords:
Sensitive Data Masking, OCR, NLP, Privacy Protection, Secure File Upload, Data Compliance

An Explainable WGAN-GP Framework for Deepfake Voice Detection

Mrs. S.Sahebzathi, T.Aruna, T.Praveena, A. Al kabeeba

Department of Computer Science and Engineering, Velammal College of Engineering and Technology, Tamilnadu, India
Correspondence: 23csec18praveenathirumalai@gmail.com

Abstract

The fast progress of speech synthesis and conversion technology has significantly increased the risk of audio deepfake misuse in fields such as fraud, impersonation, and misleading information. Traditional detection algorithms based on handmade acoustic characteristics frequently fail to generalize to newer generative models. In order to address these issues, our study provides a hybrid synthetic speech detection system that combines WGAN-GP with Grad-CAM. Mel-spectrogram representations are implemented to capture the discriminative time-frequency features of speech signals, while WGAN-GP supports stable adversarial training and improved resilience towards unseen synthetic voices. Grad-CAM has been added to provide visual explanations for model decisions, which improves interpretability and forensic validity. Experimental assessment on various benchmark datasets shows up to 94% detection accuracy, better cross-dataset generalization, and useful visual insights into spectro-temporal areas crucial for categorization. The findings show that the suggested design provides a reliable and applicable approach for real-world synthetic detection of sounds applications.

Keywords:
Synthetic Voice Detection, Audio Deepfake, WGAN-GP, Grad-CAM, Explainable AI

Quantum-Resistant Cryptography for Secure IoT Communication Systems

Aakash S 1, Kalish S 1, Nivetha S 2

1 CSE with Cybersecurity, Sathyabama Institute of Science and Technology, Chennai, India
2 Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India
Correspondence: nivetha.s.cse@sathyabama.ac.in

Abstract

The rapid expansion of Internet of Things (IoT) ecosystems has increased the need for communication mecha-nisms that can remain secure against emerging computational threats. Conventional asymmetric cryptographic schemes, includ-ing RSA and Elliptic Curve Cryptography (ECC), are vulnerable to advances in quantum computing due to the ability of Shor's algorithm to undermine their underlying mathematical assumptions. To address these challenges, this paper presents PQ-IoT SecureCom, a quantum-resistant communication frame-work built using NIST-standardized post-quantum cryptographic primitives. The proposed framework employs ML-KEM (derived from Kyber) for secure key encapsulation and ML-DSA (derived from Dilithium) for digital authentication, combined with AES-GCM to ensure data confidentiality and integrity. Additional security mechanisms, including PQC-based device certification, periodic session key updates, and nonce-based timestamp val-idation, are incorporated to mitigate replay and impersonation attacks. The framework also supports a hybrid operational mode that enables performance comparison between classical and post-quantum cryptographic schemes. System behavior is monitored using a real-time dashboard that records cryptographic overhead, communication metrics, and detected security events. Experimental evaluation shows that ML-KEM and ML-DSA significantly enhance security while introducing computational overhead that remains acceptable for contemporary IoT devices. Through automated attack simulations and detailed event logging, PQ-IoT Secure Com demonstrates the practical feasibility of deploying scalable post-quantum security in IoT communication systems.

Keywords:
Post-Quantum Cryptography, IoT Security, ML-KEM, ML-DSA, Hybrid Cryptography, MQTT, Digital Signa-tures, Replay Protection, Lattice Cryptography

A miniaturized frequency reconfigurable Antenna for sub-6 ghz 5g and WBAN Communications

Vignesh M 1, Arulmurugan S 1, Minakshmi Shaw 2, Pradeeksha P V 3,
Sobika A K 3, Sarveshwaran J 3

1 Department of Electronics and Communication Engineering, Kongu Engineering College, Perundurai, Erode, Tamil Nadu, India.
2 School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India.
3 Department of Electronics and Communication Engineering, Kongu Engineering College, Perundurai, Erode, Tamil Nadu, India.
Correspondence:sarveshwaranj.22ece@kongu.edu

Abstract

A frequency reconfigurable antenna operateing at 3.3 GHz and 5.8 GHz is investigated using RF PIN diodes. The antenna consists of two rectangular patches divided by a narrow gap. This configuration enables frequency switching via PIN diode bias control. Depending on the diode biasing the antenna can switch efficiently between 3.3 GHz 5G communication and 5.8 GHz, for WBAN communication. Simulation outcomes validate performance throughout the switching operation. The reconfigurable antenna provides a peak gain of 2.42 dBi at 3.3GHz (ON State). 6.9 dBi at 5.8GHz (OFF state). It offers impedance bandwidth of 4.7% at 3.3 GHz in the ON mode (155 MHz) and 3.31% at 5.8 GHz, in the OFF mode (192 MHz) demonstrating consistent bandwidth performance in both states. This design suits wireless communication systems, particularly Wireless Body Area Networks (WBAN) and sub-6 GHz 5G implementations. These results show stable radiation characteristics with acceptable gain at both frequencies.

Keywords:
Frequency Switching, Reconfigurable Antenna, PIN Diode, WBAN.

Military Digital Twins - A Data-hardened Architecture for Digital Twins to Enable Operational Resilience in Adversarial Environments

Anand Rath, Manas Ranjan Patra

ML Engineering Consultant to Process Engineering Industry, Former Researcher, ABB Corporate Research, Bangalore
Department of Computer Science and Engineering, NIST University, Berhampur
Correspondence: mrpatra@nist.edu

Abstract

We propose a data-hardened architecture for military digital twins that can enable resilient, integrated warfare under contested environments. We first elicit the foundational requirements of a military digital twin and use them to derive its defining architectural choices. Designed explicitly for adversarial environments, it adopts a zero-trust posture in every design decision and employs Bayesian consensus mechanisms to build trust dynamically over time, enabling battlefield assets to verify one another for signs of compromise. Furthermore, the architecture mitigates the challenges of intermittent, low-bandwidth connectivity at the edge by employing a hybrid construct: a lightweight, low-fidelity edge twin paired with a high-fidelity command-center twin. This division of labour enhances resilience, maintains operational continuity, and strengthens the overall robustness of the military digital twin ecosystem.

Keywords:
Digital twin, data resilience, DDIL, machine learning, Bayesian networks, trust model, tactical edge, contested environment, uncertainty

Detection of Coordinated Social Media Manipulation using Temporal Network Analysis

Ramya D, Vishali M, Dhora M, Meena R, Bowyashree K,

Department of Computer Science and Business Systems, Sri Eshwar College of Engineering, Coimbatore, India
Correspondence: bowyashree.k2023csbs@sece.ac.in

Abstract

Social media platforms have been more frequently targeted by a concerted effort in manipulation campaign in order to influence opinions and misinform as well as artificially amplify stories. Current detection methods tend to use network characteristics or content information that are static and do not detect the dynamic and cooperative behavior of coordinated inauthenticity. This paper suggests a framework based on temporal network analysis of identifying coordinated social media manipulation through modeling user interactions as time-evolving graphs. The framework combines temporal edge-construction, synchronized activity-detection, and community-level coordination measures in order to find collections of accounts that perform in a coordinated fashion. Two publicly available data sets of social media containing confirmed manipulation campaigns and organic interactions with users are experimented with. The proposed approach has a F1-score of 0.91, precision of 0.93 and recall of 0.89, which is 8-14 times higher than the state-of-the-art baseline methods such as static graph clustering, bot-detection models and content-based classifiers. The analysis of temporal motifs shows that the coordinated manipulation accounts have a much higher interaction synchrony and repeated patterns of activation than genuine users. The proposed framework also shows a high level of generalization across platforms, and performance deterioration under 4% when tested on unseen data. The findings affirm that use of temporal dynamics is important in order to detect coordination manipulation campaigns. The suggested strategy is a platform-agnostic early warning of organized influence operations, and the proposed strategy can be applied practically to reduce misinformation, control platforms, and build digital trust.

Keywords:
Social Media Manipulation, Coordinated Inauthentic Behavior, Temporal Network Analysis, Information Diffusion, Misinformation Detection

Strategic Information Confrontation Through Persistent Digital Surveillance: An Integrated OSINT-Social Engineering Framework for Long-Term Intelligence Weaponization

Abinash Kumar Pala 1, Raghunandan Swain 2, Manish Tripathy 2, Dinesh Kumar Dash 2, Priyadarsan Patra 1, Sandipan Mallik 1

1 Dept. of ECE, NIST University Berhampur, India
2 Dept. of ETC, Prala Maharaja Engineering College (BPUT, Odisha), Berhampur, India

Correspondence: sandi.iitkgp@gmail.com

Abstract

In the age of security around data and machine learning, it is important to protect that data while enabling means to effectively analyze it. This paper proposes a secure framework that combines cryptographic data protection with deep learning techniques, allowing meaningful knowledge extraction without sacrificing data security. A CMAP authentication protocol is proposed for securing data exchange on federated cloud servers and brings together cryptography, machine learning, and statistical models to contextualize data. The cryptographic algorithm selected for data exchange was the DES (Data Encryption Standard) algorithm for encryption. Data preparation for neural network and deep learning processing included techniques such as one-hot encoding, tokenization, stemming, stop-word removal, and normalization. The various available deep learning models (CNN, LSTM, and GRU) were evaluated for predictive analysis and data classification; the data was defined as binary to ensure compatibility with numerous machine learning algorithms. This paper highlights that merging cryptographic algorithms with machine learning is achievable while positively affecting the relationship between data privacy and analysis.

Keywords:
Encrypted Text, deep learning, cryptography, CMAP, LSTM, Bi-LSTM, DE

Transforming Text into Secure Information: A DES Encryption and Deep Learning Approach

Rahul Kumar 1, Kirti. Kumari 2, Ch Sree Kumar 3, Manjushree Nayak 4, Brojo Kishore Mishra 5, Sandipan Mallik 6

1 International Institute of Information Technology-Hyderabad (IIIT-H), India
2 Indian Institute of Information Technology Ranchi, Ranchi, India
3 SRM University, Andhra Pradesh, Amaravati, India
4 Amity University, Chhattisgarh, India
5 Department of CSE, NIST University, Berhampur, Odisha, India
6 Department of ECE, NIST University, Berhampur, Odisha, India
Correspondence: sandi.iitkgp@gmail.com

Abstract

In the age of security around data and machine learning, it is important to protect that data while enabling means to effectively analyze it.This paper proposes a secure framework that combines cryptographic data protection with deep learning techniques, allowing meaningful knowledge extraction without sacrificing data security. A CMAP authentication protocol is proposed for securing data exchange on federated cloud servers and brings together cryptography, machine learning, and statistical models to contextualize data. The cryptographic algorithm selected for data exchange was the DES (Data Encryption Standard) algorithm for encryption. Data preparation for neural network and deep learning processing included techniques such as one-hot encoding, tokenization, stemming, stop-word removal, and normalization. The various available deep learning models (CNN, LSTM, and GRU) were evaluated for predictive analysis and data classification; the data was defined as binary to ensure compatibility with numerous machine learning algorithms. This paper highlights that merging cryptographic algorithms with machine learning is achievable while positively affecting the relationship between data privacy and analysis.

Keywords:
Encrypted Text, deep learning, cryptography, CMAP, LSTM, Bi-LSTM, DES

Quantifying Narrative Dominance: The Authenticity Trap and Data-Driven Decision Support in Cognitive Warfare

Nishank Sharma

Department of CSE, Indian Institute of Technology Indore, Indore, India
Correspondence: mt2502193020@iiti.ac.in

Abstract

Present day conflicts around the globe have proved that it is not only the kinetic domain that matters for decision matrix, but also several non kinetic factors also steer much of pioneer decision making. While traditional intelligence frameworks remain glued to correctness of data and its authenticity, here we would like to re-contest that this practice creates a critical void and deep overlooking vulnerability, we coin this term as 'AUTHENTICITY TRAP'. Non-kinetic Warfare, especially cognitive space warfare (CW), weaponizes these blind spots by populating social channels with fake, immaterial, blind contents that, while logically, socially, and technically inauthentic, drive genuine and often destabilizing behavioral changes in masses and targeted populations. Therefore, to address this void, we introduce the Social Domain Scrutiny Engine (SDSE) and a key term called the Divergence Index (Di). With our analysis of our dataset, which we name "Operation Azure," and our reconstruction of recent geopolitical crises from 2019 to 2024, we here demonstrate that filtering out unwanted, adversarial noise results in a 48-to-72 hour latency in threat detection. Conversely, our SDSE model successfully demonstrates and predicts kinetic escalation by interpreting this divergence D not as an error, but as a critical information signal.

Keywords:
Non-kinetic warfare, Cognitive Warfare, Narrative Dominance, Divergence Index, Intelligence voids, Social Domain Scrutiny, Decision Support Systems, Strategic Surprise.

Learning-Driven Wi-Fi Intrusion Prevention Using Anomaly Detection and Attack Classification

Sahil Sharma, Teek Parval Sharma

Department of CSE, National Institute of Technology, Hamirpur, India
Correspondence: teek@nith.ac.in

Abstract

Due to the growing use of IEEE 802.11 wireless networks has significantly expanded the cyber attack surface, making Wi-Fi infrastructures prime targets for protocol level ex- ploitation, traffic manipulation, and denial-of-service campaigns. Even though a lot of current methods focus on intrusion de- tection, they frequently lack the automated response capabilities needed for defensive cyber operations in real time, especially against attacks that are novel or adaptive. In order to facilitate both precise threat detection and proactive mitigation, this paper introduces a learning-driven Wi-Fi intrusion prevention framework that combines anomaly-aware traffic analysis with multi-class attack identification. The system uses a supervised classifier to distinguish between various known Wi-Fi attack categories after using an unsupervised learning component to model normal wireless behaviour and reveal anomalous activity. A lightweight decision and enforcement mechanism translates detection outcomes into immediate defensive actions, enabling rapid containment of malicious activity at the network level. A realistic Wi-Fi traffic dataset with thirteen different attack types and typical traffic is used to test the framework. The experimental results show a 99.29% detection accuracy, a 99.61% detection rate, efficient detection of zero-day attacks, and low processing latency appropriate for real-time deployment. The findings show that the suggested system improves defensive response and situational awareness, supporting robust Wi-Fi security in disputed cyber environments.

Keywords:
Wi-Fi security, Intrusion prevention system, Anomaly detection, Machine learning, Defensive Cyber Operations.

SAKSHI: Agentic AI for Regional Intelligence using Structured Open-Source Intelligence (OSINT)

Nishank Sharma 1, Surya Prakash 1, Hemprasad Patil 2

1 Indian Institute of Technology (IIT) Indore, Indore, India
2 Military College of Telecommunication Engineering Mhow, Indore, India
Correspondence: hemprasadpatil@gmail.com

Abstract

Globally, most security domain analysts are facing a heterogeneous challenge: keeping pace with the fluidity and dynamic speed of geopolitical events of global importance. The highly change-led, fluid nature and overwhelming magnum of Open-Source Intelligence (OSINT) many times render manual processing insufficient. Traditional methods struggle to maintain a coherent and consistent operational picture across disparate regions, mainly missing subtle but critically important connections—such as minor kinetic skirmishes in one sector triggering economic ripples in another section that presage a broader escalation. So, in this paper, we introduce the Strategic Awareness Knowledge System for Heuristic Information (SAKSHI), an intelligent framework designed to augment the human cycle of analysis and information interpretation. As SAKSHI continuously ingests information, it maintains an organized historical record and autonomously identifies various emerging patterns. Therefore, by using a transformer-based reasoning engine, it is able to detect concerning security events; also, it uncovers various hidden cross-domain linkings by using a timelag correlation mechanism and further tracks regional instability metrics. We have carried out a 100-day evaluation; the system has successfully identified hidden undercurrent relationships between geopolitical factors and generated concise reports of escalation risks, yielding an F1 accuracy score of 0.84. Inherently, these findings suggest that SAKSHI offers a visible and confident advantage in deciphering entangled, complex security landscapes.

Keywords:
Open-Source Intelligence (OSINT), Agentic Artificial Intelligence (AI), Structured Memory, Cross-domain Correlation, Geopolitical Risk

LSTM based Threat Intelligence Methods for Intrusion Classifications of DOS Attack in WSN

Bipin Bihari Jayasingh, M Yogitha

IT Department, CVR College of Engineering, Hyderabad, India.
Correspondence: mittayogitha123@gmail.com

Abstract

Wireless Sensor Networks (WSNs) are becoming more common in various applications such as environmental monitoring, military applications and health care networks. Because WSNs are often resource-constrained and operate over a channel of open communication, these networks have some significant security implications. Among these security implications, Denial of Service (DoS) attacks pose a significant threat to the availability of a network by disrupting normal operation and degrading data integrity. Effective cybersecurity strategies are necessary to defend against DoS attacks, and denial of service threat intelligence methods would require mechanisms that can discover attack signatures as well as anomalous behaviors in real-time. In this paper, we present an Intrusion Detection System (IDS) based on deep Learning which uses LSTM networks to detect and classify DoS attacks. The benefits of the LSTM framework are identified as the structures ability to depict or capture temporal patterns in network traffic sequences and gives the benefit of identifying complex and dynamically changing behavior patterns over time. Finally, By leveraging threat intelligence and implementing sound cybersecurity strategies, our system improves the defensive capability of the network to both sophisticated and adaptive attacks. The proposed IDS has been both trained and tested on the WSN-DS dataset which contains multiple attack classes including Normal, flooding, and TDMA attacks.

Keywords:
Wireless Sensor Networks, Intrusion Detection System, Long Short-Term Memory, Denial of Service attacks, Deep Learning, Attack classification.

A Real-Time Drone Detection System using Hybrid Deep Learning YCFANet

Siba Sundar Das, Sai Krishna Beeraka, Charulata Palai, Pradeep Kumar Jena*

Department of CSE, NIST University, Berhampur Odisha-761008
Correspondence: pradeep@nist.edu

Abstract

The timely detection of low-altitude aerial threats is a critical requirement in modern air-defense and security operations. Small and fast-moving unmanned aerial vehicles (UAVs), particularly drones, pose significant challenges to conventional surveillance systems due to their limited visual signatures, high mobility, and susceptibility to environmental variations. This paper presents YCFANet, a hybrid deep learning framework designed for real-time drone detection in UAV imagery, with a specific emphasis on airspace surveillance and early warning applications. The proposed framework is built upon a YOLOv8 backbone and integrates weather-aware data enhancement techniques to improve robustness under diverse illumination and atmospheric conditions. To strengthen the localization of small and dynamic aerial targets, the standard YOLO neck and detection head are replaced with a CBAM-enhanced SlimNeck and a multi-branch FRMHead, respectively. Additionally, an adaptive focal loss is employed to mitigate class imbalance and enhance detection reliability for drones compared to other airborne objects, including airplanes, helicopters, and birds. Experimental results demonstrate that YCFANet achieves a drone detection accuracy of 95.9% and an overall average accuracy of 96.8% across all classes, while sustaining a real-time processing speed of 24.7 frames per second. Both quantitative evaluations, including confusion matrices and precision–recall curves, and qualitative analyses confirm stable performance under occlusion, motion blur, and adverse weather conditions. These findings indicate that YCFANet can function effectively as an AI-based perception module for UAV-assisted aerial surveillance and defense-oriented threat monitoring systems.

Keywords:
Drone Detection, Unmanned Aerial Vehicle (UAV), Small Object Detection, YOLOv8 Backbone, Hybrid Deep Learning (YCFANet), Real-Time Surveillance .

Operation Sindoor: Role of the Indigenous Integrated Air Command and Control System (IACCS) in a High-Tempo Network-Centric Conflict – A Case Study

Niranjan Kumar Parhi

Director & CEO, PN CyberTrust Technology Private Limited, Bhubaneswar, India,
Correspondence: nkparhi13@gmail.com

Abstract

The increasing complexity and tempo of contemporary air operations necessitate integrated command-and-control systems capable of fusing heterogeneous sensor inputs, supporting distributed decision-making, and enabling coordinated execution across multiple operational echelons. This paper presents a systems-oriented analysis of India's Indigenous Integrated Air Command and Control System (IACCS) and examines its role during Operation Sindoor, a limited-duration, high-intensity conflict scenario in May 2025. The study deliberately avoids classified or tactical disclosures and instead focuses on architectural principles, functional integration, and system-level performance characteristics derived from open-source information and doctrinal analysis. The paper evaluates how IACCS supported real-time situational awareness through multi-sensor data fusion, enabled decentralized yet synchronized command-and-control across multiple operational echelons, and enhanced operational resilience in contested and time-critical environments. Key system attributes, including scalability, latency management, redundancy, interoperability, and human–machine interaction, are examined from a systems engineering perspective. The findings indicate that indigenous, modular C4ISR architectures could significantly compress decision cycles and improved joint-force coordination in the limited conflicts. By framing IACCS as a system-of-systems rather than a platform-centric solution, this paper contributes to the broader literature on sovereign defense technologies, network-enabled operations, and command-and-control system design

Keywords:
IACCS, Human–machine interaction, Modular C4ISR architecture

Platform Power and National Security Doctrine

L. C. Patnaik

Professor Emeritus, Rashtriya Raksha University
Correspondence: lcpatnaik@gmail.com

Abstract

This paper defines platform power as the capacity to design, govern, and assure digital Infrastructures clouds, satellites, data fabrics, and algorithmic systems—that enable sensing, communication, computation, and decision-making in contested environments. We develop a seven-layer Platform Security Stack (PSS) and compare two archetypes: the United States' orchestrated openness, which integrates private hyperscalers and commercial space into defence through contractual governance, and China's integrated control, which fuses state-led platforms under civil–military fusion (MCF). Drawing lessons for India, we propose a National Platform Security Doctrine (NPSD) emphasising multi-cloud assurance, sovereign PNT, dual-use acceleration, platform continuity law, and cognitive security. The contribution is a doctrine-level framework that aligns technical controls with legal instruments and alliance interoperability. The conclusion outlines a 2035 outlook in which India helps shape a democratic technology order through trusted standards and exportable digital public goods.

Keywords:
Platform Power; Digital Sovereignty; National Security; PNT; Cloud; AI; Civil–Military Fusion; DPR; Cognitive Security; India.

Study Of Propellants For Muzzle Velocity Enhancement In Medium Caliber Gun Ammunitions

Durlav Swain 1, Deepak Govindraj 2, Nagendra Kumar 3 & Rajagopal Chellamani Srikanth 4

1,4 Army Air Defence College, India
2,3 Department of Aerospace, Indian Institute of Technology Bombay, India
Correspondence: durlav.swain@gmail.com

Abstract

The paper is focused on the enhancement of muzzle velocity for small and medium caliber gun ammunitions, typically those used by Army Air Defence, with an aim to cater for present day highly agile and small air targets such as Drones and Unmanned Aerial Systems. The paper covers the design aspects of lab feasible and institutionally permissible, gun barrel along the requisite sub parts and accessories which could facilitate testing of gun propellant performance, in terms of chamber pressure generation and muzzle velocity achieved. The paper includes experimental test results on five types gun propellants with different composition primarily Nitrogen rich materials, which channelised the way forward for further research work.

Keywords:
Gun Propellant, Chamber Pressure, Muzzle Velocity, Force Constant, Adiabatic Temperature.

Passive Detection System : De-Novo Look

Himanshu Chaudhary, Ayush Mudgal, Manoj Kumar Yadav, Rajagopal Chellamani Srikanth

Army Air Defence College, India
Correspondence: himanshuc129@gmail.com

Abstract

Modern warfare increasingly relies on the ability to sense, track and interpret adversary activities without revealing one's own presence. Passive Detection Systems (PDS) have emerged as a niche yet disruptive capability, enabling forces to detect, classify and localize targets by exploiting adversary emissions or environmental disturbances rather than active transmissions. Defence establishments worldwide are investing in passive radar, passive sonar, Electronic Support Measures (ESM), Infrared/ Optical Sensing, Acoustic and Seismic Sensor networks and space-based passive surveillance to counter stealth aircraft, low-observable UAS, cruise missiles and network-centric operations. These systems offer advantages such as enhanced survivability, resistance to electronic attack and jamming, and covert situational awareness, while also posing challenges related to sensor fusion, data processing, and integration into existing command and control architectures. This paper surveys contemporary developments in passive detection technologies globally and examines India's progress in this domain.

Keywords:
Passive Detection Systems (PDS), Passive Radar, Multistatic Radar, Air Defence Surveillance, Electronic Warfare(EW), Electronic Support Measures (ESM), Low Observable Targets, Multisensor Data Fusion, RF Interferometry, InfraredSensor, Electro-Optical Sensors, Counter-UAS Systems.

Electronic Fratricide in Air Defence Operations While Countering UAS In Tactical Battle Areas

M Y Khan, Pranjal Agarwal & Rajagopal Chellamani Srikanth

Army Air Defence College, India
Correspondence: mohhan.792f @gov.in

Abstract

Electronic fratricide in air defence operations refers to the unintended interference, degradation or neutralisation of friendly sensors, communication networks, navigation aids and weapon control systems due to uncoordinated electronic emissions within a contested electromagnetic environment. Therapid proliferation of Unmanned Aerial Systems (UAS),operating across diverse frequency bands with low radar cross-sections, has compelled air defence forces to increasingly rely onelectronic countermeasures, jammers, spoofers and directed energy weapons[1][2]. While these measures are essential for countering hostile UAS, inadequate spectrum coordination and decentralised control can inadvertently disrupt friendly systems, resulting in loss of situational awareness, delayed engagements and increased risk of blue-on-blue incidents[2][4]. This paper analyses the evolution of the UAS threat, its employment in contemporary conflicts, existing counter-UAS measures and the primary causes of electronic fratricide. Case studies from recent conflicts are examined to highlight operational risks, followed by recommendations to mitigate electronic fratricide through centralised command and control, integrated spectrum management, training and procedural reforms.

Index Terms:

Electronic Fratricide, Air Defence, Unmanned, Aerial Systems, Electronic Warfare, Counter-UAS.

Sensitivity Enhancement of Quantum Radar Using Entangled Single Photon Source for Military Defense Security

Simanchalo Panigrahi, Tejaswini Patro

Department of Physics, NIST University, Odisha, India
Correspondence: simanchalopanigrahi@nist.edu

Abstract

Quantum radar represents a promising advancement over classical radar systems by exploiting quantum mechanical phenomena such as entanglement and quantum measurement to overcome fundamental detection limitations. This paper reviews the evolution of radar technology from conventional radar frequency systems to quantum radar architectures, with emphasis on sensitivity enhancement and detection of RF-stealth targets for military defense applications. Classical radar parameters such as radar range, transmitted power and cross section are revisited and extended to their quantum analogues. The role of entangled single photon sources in improving detection performance under high noise and jamming environments is discussed. Context of microwave quantum radar is reviewed along with photonic implementations. This paper further highlights the importance of quantum measurement theory, including system-apparatus entanglement, density matrix formalism and wave function collapse in extracting information from quantum radar systems. Although significant experimental challenges remain, recent advances indicate strong potential for future development of quantum radar in next generation defense and surveillance systems.

Keywords:
Quantum radar, entangled single photon, quantum measurement.

Niche and Disruptive Technologies in Defense and Security

Saurabh Sanwal, Manoj Kumar Yadav & Rajagopal Chellamani Srikanth

Army Air Defence College, India
Corresponds: saurabhsanwal.456f@gov.in

Abstract

Modern Warfare is being transformed by niche anddisruptive technologies – specialized, cutting-edge innovations can render traditional systems obsolete[1][2]. Across theglobe, defence establishments are investing heavily in domainstactical UAVs[4]. An Indian perspective is included: from India'sDRDO labs and emergent unmanned units to hypersonic missiletests and space assets (e.g. 2024 ASAT test). Strategicimplications are also discussed (e.g. arms race, deterrence,ethical concerns) and policy initiatives (NATO's tech strategy[2],India-Russia cooperation on "niche" systems[5]). The paper concludes by outlining a pragmatic roadmap for leveraging nichetechnologies to enhance defence preparedness, operational such as Artificial Intelligence (AI), Autonomous Systems(Unmanned Vehicles and Robots), Quantum Technologies,Biotechnology, Hypersonic Weapons, Directed-Energy Weapons(Lasers/ Microwaves) and advanced materials. These emergingfields promise enhanced situational awareness, decision-speedand asymmetric advantages, but also pose new strategic challenges. This paper surveys the latest disruptive defencetechnologies worldwide and examines India's efforts to adoptthem. Real-world examples are highlighted: for instance, U.S.forces trialed a 60 kW naval laser to shoot down a drone[3] andUkraine's army attributes two-thirds of Russian losses to small resilience and long-term deterrence in an increasingly contestedand technology-driven security environment.

Keywords:
Disruptive Technology, Niche Technology,Defence, Security, Artificial Intelligence, Autonomous Systems,Cyber Warfare, Quantum, Hypersonics, Directed-Energy,Biotechnology, India.

AI based Resonance Avoidance in Military Vehicle Components

Santosh Kumar Panda1, Ratikanta Nayak2

1Department of Mechanical Engineering, NIST University, Berhampur, Odisha, India, 761008
2Department of Physics, NIST University, Berhampur, Odisha, India, 761008Correspondence: ratikanta.nayak@nist.edu

Abstract

Army vehicles operate in extreme environmental conditions, making them highly vulnerable to the risk of resonance in mechanical systems. The interaction of engine excitation frequencies and terrain-induced accelerations with the system natural frequencies may result in resonance, causing amplified dynamic responses, increased material fatigue, degradation of sensing performance, and potential failure of critical components such as antenna support structures, gun barrels, and optical systems. Traditional passive vibration control techniques are inadequate for such applications due to their fixed tuning and inability to adapt to varying operational conditions.The objective of this paper is to propose a new system using Artificial Intelligence (AI) capable of not only pointing out but also countering a problem of resonance in a system. The proposed system makes use of a Fuzzy Logic Controller (FLC), which has been developed using Python's `scikit-fuzzy` library. The revolution per minute (RPM) value and vibration amplitude are selected as input variables to identify the danger of system resonance. A mathematical model of a representative vehicle component is used for the simulation of vibration behaviour and identification of resonance danger zones. The military vehicle and its components are considered as a single component during the simulation. Simulation results show that the intelligent control system is able to detect an increase in the vibration level by avoiding resonance; this leads to improved durability of components and overall reliability in military applications.

Keywords:
Active Vibration Control, Fuzzy Logic Controller, Resonance Avoidance, Military Vehicles, Structural Health, Intelligent Control Systems

Cyber Takeover of UAS - Opportunities and Challenges

Vipin Kumar Singh*, Shubham Pandey & Rajagopal Chellamani Srikanth

Army Air Defence College, India
Corrosondence: vipinpesce@yahoo.co.in

Abstract

Unmanned Aerial Systems (UAS) have penetrated both civil and military fields due to their flexibility, autonomy and cost effectiveness. However, this reliance has exposed UAS to sophisticated cyber takeover risks, where adversaries exploit vulnerabilities in communication links, navigation systems and control protocols. Recent conflicts demonstrate both the opera-tional potential and the security challenges of UAS showcasing both autonomous capabilities and vulnerabilities to electronic interference. Additionally, widespread use of GPS jamming and spoofing on the battlefield has underscored the susceptibility of UAS to cyber-electronic disruption and hostile takeover attempts.

These developments highlight opportunities for enhancing mis-sion resilience through secure communications, autonomous de-cision algorithms and intrusion detection systems, alongside the challenge of defending against adversarial electronic warfare and software exploitation. This paper surveys these dual facets, draw-ing on recent conflict cases to review cyber takeover opportunities and challenges in modern UAS operations [1].

Keywords:

Unmanned Aerial Systems, Cyber Takeover, Electronic Warfare, GPS spoofing, intrusion detection.

Air Littoral: An Emerging Concept for Land Forces

Aditya Beniwal

Tactics & Combat Wing Army Air Defence College Gopalpur, India
Correspondence:addybeniwal@gmail.com

Abstract

Modern land warfare is increasingly shaped by the contested low-altitude battlespace known as the air littoral, extending from the surface to approximately 10,000 feet. This paper examines how the proliferation of low-cost unmanned aerial systems, loitering munitions, and electronic warfare has redefined air superiority and blurred traditional boundaries between land and air operations. Drawing lessons from recent conflicts such as the Russia–Ukraine war, Nagorno-Karabakh conflict, and Operation Sindoor, the study highlights doctrinal, organizational, and technological implications for joint force employment and airspace control.

Keywords:
Air Littoral, Unmanned Aerial Systems, Counter-UAS, Joint Operations, Airspace Control, Modern Warfare

DRAMS : Threat & Role of Ground Based Air Defence Weapon System

Siddharth Baloni, Anmoldeep Bhullar, Vipin Kumar Singh, Shubham Pandey & Rajagopal Chellamani Srikanth

Army Air Defence College, India
Correspondence: siddharthbaloni@gmail.com

Abstract

Drones, Rockets, Artillery, and Munition Systems (DRAMS) have fundamentally transformed modern battlefields through coordinated saturation attacks that overwhelm traditional air defense systems. Recent conflicts including the Armenia-Azerbaijan conflict (2020), Russo-Ukraine operations (2022-2025),Israel-Iran confrontation (June 2025) and Operation SINDOOR (May 2025) demonstrate DRAMS' decisive operational impact. Critical challenges in detection, tracking and interception of low-RCS platforms are identified across multiple threat brackets-low altitude(0-10,000 feet), medium altitude (10,000-30,000 feet)and deep envelope (above 30,000 feet). Ground Based Air Defence Weapon Systems (GBADWS) have transitioned from protective shields to critical enablers of combat power, demanding evolution into integrated,AI-enabled multi-layered architectures combining kinetic and non-kinetic effectors with resilient command and control networks. The paper analyzes DRAMS threat evolution, manifestations in recent conflicts and environment scan of Counter-DRAMS capabilities. Recommendations emphasize multi-sensor fusion, indigenous Directed Energy

Weapons (DEW)development, quantum-secure C2 architecture and organic Counter-UAS capabilities. Establishment of multi-layered AD architecture, AI-enabled sensor fusion and integration across services as a central pillar are identified as essential for future operational dominance in contested airspace.

Keywords:
DRAMS, GBADWS, Counter-UAS, Loitering, Munitions, Directed Energy Weapons, Electronic Warfare, Air Defence, Sensor Fusion, Quantum, Technologies, Counter-DRAMS, India.

Evolving Air Threat: Impact of Technological Upgrades in Field of Avionics, Sensor to Shooter Linkages, BVR & Stand Off Capabilities and Extensive Proliferation of UAS

Sachidanand Dwivedi

Army AD College, Gopalpur, India.
Correspondence: a449dwivedi@protonmail.com

Abstract

The contemporary air threat environment is undergoing fundamental transformation driven by advances in avionics,proliferation of precision stand-off weapons systems, and the rapid maturation of unmanned aircraft / systems across the conflict spectrum clubbed with modern sensor fusion, network-centric architectures. The traditional air defence concepts and legacy air defence systems face critical obsolescence if modernization efforts do not match the pace of threat evolution. Strategic implications of the evolving hybrid aerial threat which encompasses variety ofvectors ranging from fifth generation aircrafts to small sized Unmanned Aerial Systems (UAS) are extensive, including compression of decision timelines at all levels, profound deterrence challenges, economic vulnerability to cost-imposition strategies, and particular relevance to regional security dynamics. The paper aims to bring out aspects of evolved air threat in view of technological upgrades and assess its manifestation in the recent US operation in Venezuela.

Keywords:
UAS, BVR, Network centric architecture

Strategic Environment and Geopolitical Shift - Artificial Intelligence, Cyber Resilience and the Architecture of Air and Missile Defence in 2026

Rajendra Kumar Yadav

Army Air Defence College, Gopalpur, Odisha, India
Doctoral Research on Defence Public Private Partnership
Correspondence: ranveerniks@gmail.com

Abstract

The international security environment of 2026 is shaped by a convergence of artificial intelligence (AI), cyber power, space systems, and the erosion of traditional deterrence frameworks. Military power is no longer defined primarily by platforms such as aircrafts, tanks, or warships, but by the ability to control data, algorithms, and digitally networked battlespaces. This transformation has profound implications for air and missile defence (AMD), where low-cost autonomous systems, cyber-enabled disruption, and precision-guided missiles now threaten even the most advanced forces. This paper integrates two analytical perspectives: first, the global shift from hybrid warfare to algorithmic warfare, and second, India's strategic response through Atmanirbhar Bharat, defence public-private partnerships (PPPs), and indigenous Integrated Air and Missile defence (IAMD). By examining initiatives such as Project Kusha, Mission Sudarshan Chakra, and Operation Abhyaas (2025), the paper argues that future deterrence will depend less on retaliatory firepower and

more on technological sovereignty, system resilience, and civil– military integration. It proposes a "Whole-of-Nation Air Defence" framework in which algorithms, networks, industry, and society become as critical as missiles and radars.

Keywords:
Artificial Intelligence, Algorithmic Warfare,Integrated Air and Missile Defence (IAMD), Cyber Resilience, Project Kusha, Operation Abhyaas, Defence Diplomacy, Atmanirbhar Bharat, C4ISR, Public-Private Partnerships.

Technological Innovation & Future Security- Impact of Supersonic and Hypersonic Weapon Systems on Air and Missile Defence

Alok Pratap Singh

Army Air Defence College Gopalpur, Odisha, India
Correspondence: alokpratap1987@yahoo.com

Abstract

The rapid advancement of supersonic and hypersonic weapon systems, exceeding Mach 5 with unpredictable maneuverability, fundamentally challenge Air and Missile Defence (AMD) architectures globally. For India, facing asymmetric threats from China's operationalized DF-17 hypersonic glide vehicle fleet (~100 deployed systems) and Pakistan's emerging hypersonic capabilities via Chinese CM-400AKG technology transfer, these systems amplify strategic vulnerabilities despite indigenous technological progress.India's January 2026 HSTDV scramjet combustor breakthrough—achieving 12-minute sustained burn at Mach 5+conditions—validates air-breathing hypersonic propulsion and positions the nation as Asia's emerging hypersonic power. However, current air defense systems (S-400 Triumf at 400 km range, Akash-NG at 45 km, Barak-8 MRSAM at 70 km) face critical detection, tracking, and engagement gaps against maneuvering hypersonic threats that compress response timelines to 5-15 minutes. This paper examines technological characteristics, evaluates strategic implications, and proposes integrated defense innovations essential for India's security posture. Recommendations include accelerated BrahMos-II (Mach 8, 1,500 km range) development, space-based sensorconstellation expansion via ISRO, Project Kusha hypersonic interceptor advancement, AI-enabled command architecture deployment, S-500 system acquisition, and QUAD coalition partnerships leveraging allied sensor networks and Hypersonic and Ballistic Tracking Space Sensor (HBTS) integration.

Keywords:

Hypersonic weapons, HSTDV, BrahMos-II, scramjet technology, India defense, S-400, Akash missile, Project Kusha, strategic stability, QUAD cooperation, space based sensors.

Multi-Sensor Intelligence Fusion for Real-time Airspace Security

Lt Col Prashant Katoch, Prof Rama Rao Nidamanuri

Indian Institute of Space Science and Technology, Thiruvananthapuram, Kerala, India
Correspondence: prashantkatoch@gmail.com, rao@iist.ac.in

Abstract

The complexity of modern airspace is increasing, as it becomes more congested and contested with high volumes of information flowing through it. Increasingly, conventional air surveillance systems are facing challenges associated with the introduction of new technologies such as unmanned aerial vehicles (UAVs), low observable (LO) threats and electronic countermeasures. This paper investigates multi-sensor intelligence fusion technology, which will allow for the combination of diverse sensor datasets in order to provide a more comprehensive understanding of the airspace environment. The paper brings out various methods of fusion, provides examples of how they have
improved situational awareness, as well as detection and decision support capabilities and identifies challenges associated with multi-sensor intelligence fusion, such as data latency and diversified datasets. This paper presents the general study and conceptual review of architectural techniques to do real-time airspace security for multi-sensor intelligence fusion come from looking at the possibilities of operating with these techniques, the associated problems with those techniques and future areas for potential further research. The study concludes that Multi-Sensor Intelligence Fusion will be key to the development of future air
defence and airspace security systems.

Keywords:
Airspace; multi-sensor intelligence, fusion.

Battlefield 2035: Emerging Contours, Adversarial Postures and Implications for India's Capability Development

Sachin Sharma

Army Air Defence College,Gopalpur, Odisha,India
Correspondence: adonis2676@gmail.com

Battlespace of 2035 will challenge India, primarily, with Sino-Pak collusivity enmeshed with disruptive technologies aimed at achieving force and technology asymmetry. Therefore, India's preparation for this threat must be based not on an academic abstraction but in current ground operational dynamics, including recent indicators of Grey Zone aggression such as GPS Spoofing attacks. Terror Linked Blasts, Ricin recovery etc coupled with a comprehensive appreciation of Disruptive Technologies which would win wars of 2035 for us, even in scenarios based on conventional asymmetry with enemy.

Agentic Geo-Intelligence-Based Spatio-Temporal Operational Risk Analysis in Sensitive Regions

Sankalp Dwivedi, Chandresh Kumar Maurya, Hemprasad Patil

Indian Institute of Technology, Indore
Correspondence: mt2502193024@iiti.ac.in

Abstract

The combination of operational processes in sen- sitive fields leads to the emergence of incident patterns that are characterized by spatial and temporal variability, making proactive and risk-informed decision-making a very important task. While machine learning methods have shown a great ability to describe these patterns, their application is often impeded by a lack of interpretability and insufficient geographic validation. In this paper, an agentic geo-intelligence framework for spatio-temporal operational risk analysis is proposed, combining kernel density estimation of historical patterns, severity-based feature aggregation, probabilistic regression, and geographic validation using GIS within a single analytical process. The data on incidents is discretized into a lattice of spatial grid cells, which converts the task of future risk detection into a predictive classification task. The performance of the model and its geographic validity are assessed by the Global Moran's I, Local Indicators of Spatial Association (LISA), and Prediction Accuracy Index. Experimental results demonstrate that the proposed framework achieves predictive performance comparable to a Random Forest classifier while offering substantially higher interpretability and spatial coherence. The framework therefore provides a robust foundation for human-in-the-loop operational decision support in sensitive and security-critical environments.

Key words:
Agentic Geo-Intelligence, Spatio-Temporal Analysis, Operational Risk Analysis, Interpretable Machine Learning, Geographic Information Systems, Spatial Autocorre- lation, Kernel Density Estimation, Decision Support Systems

Sponsors

Exhibitors

Anadrone

BonV

DRDO

FxUAV

Keysight

BIG BANG BOOM SOLUTIONS

FLO FLY

Rhombus

International Conference on

AIR DEFENCE AND SECURITY (ICADS-26)

www.nist.edu/conference/icads-26

Connect With Us: @NISTUniversity