

## List of the Accepted Papers in ICISPD 2024

<b>Paper ID</b>	<b>Paper Title</b>
6	A Novel AI-powered System for Real-Time Financial Crime Detection
8	A Framework for Enhancing Supply Chain Management and Decentralized Identity On Blockchain Technology
11	Artificial Intelligence and Drone Application in Crime Scene Investigation: A scoping review
12	An analysis of the efficacy of the deep learning technique in the field of digital-forensics
13	An Analysis of the Security Status of Ethereum Smart Contracts: Vulnerability, Tools, and Techniques
16	Remote Access Trojan Detection Using Machine Learning and Network Traffic Analysis
17	Exploring the Future of Drone Forensics: A Systematic Study of Methods and Applications
18	Privacy-Preserving Transaction Verification in Decentralized Finance using Zero-Knowledge Proofs and Deep Learning
23	DS-AKA: Digital Signature Based Authentication and Key Agreement Protocol to Mitigate Fake Serving Network for 5G Communication Networks
28	A Study on the minds of 21st-century youths and how they are invested in gaming and its impact
33	TENDERING CCTV FOOTAGE IN EVIDENCE: PRACTICAL ASPECTS IN THE LIGHT OF NEW LAW AND RECENT CASES
34	Exploring Discrete Wavelet Transform and Spread Spectrum Techniques in Image Steganography: A Com-prehensive Review
35	SPACE : A MODERN BATTLEGROUND FOR CYBER WARFARE
39	Privacy Threat Modeling for Federated Learning
41	Cloud Forensics: Current Perspectives, Challenges and Potential Solutions

42	The Efficacy of Metadata Analysis in Detecting Deepfakes: A Forensic Perspective
44	Cyber Crime, Privacy, and Global Strategies Against Social Media Abuse Targeting Women
50	Ethics and Policy Issues in collection and preservation of Digital evidence
56	Efficient Video Deepfake Detection Using Boundary Hashing and Recurrent Neural Networks
62	Graph Neural Networks in Network Intrusion Detection: A Comparative Analysis
64	Large Language Models for Digital Forensic Investigations
65	Accelerating Natural Language Processing Models using Parallelisation to Detect Fake News
67	Forecasting of Indian Crime Data using ARIMA and Polynomial Regression
69	Digital Forensics Process and Current Trends
72	A comparative study of password strength prediction using baseline and ensemble based classifiers
75	Dark Web Surveillance and User Profiling Framework for Evidence Extraction Using OSINT
77	Enhancing Cyber Threat Intelligence by Network Forensic Analysis of Ransomware as a Service(RaaS)
78	Secret Image Sharing with Reduced Shadow Image Size without Combiner's Secret
79	A (n, n) Threshold Secret Message Sharing with Meaningful Stego-images
80	Classification of Tweets to identify Cyber-bullying Attack Based on Multi Class Classification using Machine Learning
81	EEIRS: A New Energy Efficient Design of Secure Intelli-gent Reflecting Surface Assisted GFDM-NOMA Systems
82	Unlocking Trust: A deep dive into forensics of TRON transactions through TRUST wallet
85	AKdroid: Deep Learning based Android Malware Classification using Markov Images and Text Messages
86	A novel group based authentication and key agreement protocol for Machine to Machine (M2M) communications in 5G networks
88	Performance Analysis of Quantum Machine Learning for Malware Detection
89	NAVIGATING THE DIGITAL BATTLEFIELD: STRATEGIES FOR CYBER WARFARE & NATIONAL DEFENCE

90	Evolving Institutional and Legal Standards in Digital Forensic Evidence: Balancing Privacy Rights vis-à-vis Investigative Needs
92	Enhancing Cloud-Native Security through 4C Architecture: A Comprehensive Analysis
95	Financial Security and Incident Management: A Comprehensive Review of Cryptocurrency Forensics
71	Information Privacy Protection Using Blockchain Technology For Clinical Trials Data
73	SDARAW: Sample deviation adjustment based robust audio watermarking framework
84	A CROSS SECTIONAL STUDY OF CYBER BULLYING AMONG YOUNG COLLEGE STUDENTS IN THE STATE OF ODISHA