

List of provisionally accepted papers in Fifth International Conference on Network Security and Blockchain Technology (ICNSBT-2026)	
Paper ID	Paper Title
22	A Next-Generation Cloud Storage Solution with Biometric Identity and Data Encryption
40	GuardianPi: An Edge-Based Explainable Intrusion Detection and Prevention System for IoT Networks Using BiLSTM and DistilBERT
56	PhishRL: An End-to-End Reinforcement Learning Pipeline for Automated Email Threat Triage
84	CyberBullyGuard: A Hybrid Adversarially Robust Framework for Cyberbullying Detection in Social Media Using DistilBERT
85	Adversarial Attack Detection in Software-Defined Network (SDN) using Explainable AI and Graph Neural Networks (GNN)
91	A Blockchain Based Framework for Land Registry System
94	A Secure Multimodal Biometric System Using Quantum Key-Based Cancelable Templates and Blockchain Integrity
106	A BFT-Enabled Blockchain Framework for Fraud Detection in Cross-Border Telecom Billing
112	Fog and Edge Computing in Smart Agriculture: A Study on Architectures, Security Models, and Data Management Techniques
117	Dynamic Cryptographic Algorithm Adaptation in Heterogeneous IoT-Blockchain-Cloud Environments: A Trustless Orchestration Framework
146	A Leakage-Aware Framework for Zero-Day Ransomware Detection: Classical and Quantum Machine Learning on UGRansome 2024
147	High-Integrity EHR Systems Powered by Intelligent Blockchain system.
158	A Decentralized Trust Management Framework for VANETs Using SUMO Simulation and Blockchain Smart Contracts
162	K2A-Hash: A Novel Diagonal Block Perceptual Hashing Algorithm for Blockchain-Based CCTV Video Evidence Verification
170	Cutting the Right Links: Intelligent Edge Pruning with Attention and Pattern Mining for Rumor Control
175	A Hybrid AI Model Based on Explainable Graph Transformers for Enhancing Financial Security and Operational Resilience in Banking Fraud Detection Systems
178	Temporal Visual-Semantic Graph Reasoning for Fake News Video Detection
185	Phishing URL Detection Revisited: Temporal Leakage, Benchmark Sensitivity, and SHAP-Based Dataset Bias Analysis
186	PHISHCRC: Conformal Risk-Controlled Cascades for Phishing URL Detection
187	Lightweight Certificate-Based Authentication Protocol for Vehicular Ad Hoc Networks
192	DGS-LOM: A Decentralized Group Signature Framework for Secure Blockchain-Based Land Ownership Management
197	CredChain: An Efficient Hybrid Blockchain Framework for Secure Digital Credential Verification
205	A Synergistic PSO-WOA Optimized SVD-DWT Framework for Robust Digital Image Watermarking
212	Advanced Phishing Detection in IoT: A Cloud-Assisted Hybrid Deep Learning Approach
213	HalluciGuard: A Multi-Agent Verification Framework for Explainable Hallucination Detection in Large Language Models
222	XMal-Edge: An Explainable Malware Detection and Response Framework for Edge Computing Using LLM-Augmented Ensemble Learning
227	Next-Generation Smart Traffic e-Challan Management System Powered by Blockchain
242	Homophily-Validated Feature-Similarity Graphs for GraphSAGE-Based Phishing Website Detection
243	A Crypto-Agile Zero Trust Framework for Quantum-Safe CBDC Transaction Processing Using NIST PQC Standards

Paper ID	Paper Title
244	Comparative Analysis of Hybrid Convolutional Neural Networks and Adversarial DCT Autoencoders for Trustworthy Digital Watermark Detection
246	Anomaly Detection for IoT Networks using Hybrid GAT-GCN with Dynamic Contextual Similarity and Tuned Behavioral Drift Score Analysis
252	A Robust Authentication Framework for Privacy and Security Preservation in Industrial Monitoring
258	Hybrid Machine Learning Framework for Insider Threat Detection and Response in Enterprise Systems
263	DRDS-Chain: An Adaptive Trust-Driven Explainable Federated Learning Framework with Blockchain-Verified Aggregation for Privacy-Preserving Malware and Intrusion Detection in Healthcare IoT Networks
292	Listen-and-Click: An Audio-Linked Graphical Password Scheme to Prevent Shoulder Surfing Attacks
293	Binary Classification of Malware Using Graph Convolutional and Graph Isomorphism Networks
294	A Blind Robust Image Watermarking Scheme for Copyright Protection Using Hadamard Transform and Quantization Index Modulation
295	Physiological Manifold Authentication via Normalizing-Flow Density Scoring: A Multi-Modal Contactless Biometric Framework Robust to Autonomous Adversarial Agents
297	AN IWT-DCT BASED HYBRID WATERMARKING SCHEME USING LBP FOR IMAGE AUTHENTICATION
298	A Secure Encrypted Steganographic Framework Using BLAKE3-Based Stream Encryption with LWT for Confidential Image Communication
299	Q-SCION: Reliability-First Quantum-Inspired Sine Cosine Optimisation for Latent-Space Ensemble Intrusion Detection in Smart-City Cyber Physical Systems
305	HMAC-Secured QR Payment Verification with Multi-Layer Fraud Detection for UPI Ecosystem
309	A Blockchain-Anchored Trust Verification Layer for OIDC/OAuth Misconfiguration Detection in Distributed IoT Microservice Meshes
310	Support Vector Machine (SVM) Assisted Blackhole and DDoS Attack Detection In Software Defined Wireless Sensor Networks
313	BOTA: Secure Blockchain-Assisted OTA for Resource-Constrained IoT
318	Threat-Resilient Blockchain Audit Layer for Trust Verification in Federated IoT Networks: A Security Analysis
327	Governed Cloud Data Fabric for Scalable Analytics Engineering and Intelligent Feature Lifecycle Automation
333	PhantomWeave: An AI-Driven Deception-Based Honeypot Framework with Blockchain-Based Forensic Logging
335	A Robust Approach for Secure Multi-Cloud Data Management with Privacy and Integrity Protection
337	AI-Powered Code Review Assistant: Eliminating LLM Pipeline Using AST-Enhanced Hallucination to Analyze Pull Requests Automatically
343	A Hybrid Metaheuristic Framework for Feature Selection in AI-Based Cyber Network Intrusion Detection
354	The Latency Price of Scale: A Security–Latency–Parallelism Frontier for Sharded Blockchains
357	A Lightweight and Energy-Efficient Multi-Prime RSA Algorithm using Carmichael’s $\lambda(n)$ for Resource-Constrained Devices
360	A Novel Generic Digital Circuit Based Symmetric Key Cryptography Using Session Based Key
366	Adaptive Confidence-Based Hybrid Fusion for Robust Cyberbullying Detection Using Machine Learning and Transformer Models
367	An Innovative Distance-Metrics–Guided Clustering Method for Stratifying Cardiovascular Risk in Asymptomatic Populations: A Proof-of-Concept Analysis