

A Survey on Image Cryptosystems: Combining CNN-Based Spatial Shuffling and Hybrid RSA-RC6 Cryptography

Sonam Jain¹, Dr. Chetan Gupta²

¹M.Tech. Scholar, Department of Computer Science & Engineering (Data Science),

Sagar Institute of Research & Technology (SIRT), Bhopal, India

²Assistant Professor, Department of Computer Science & Engineering,

Sagar Institute of Research & Technology (SIRT), Bhopal, India

Email: ¹sonamjain221195@gmail.com, ²chetangupta.gupta1@gmail.com

Abstract - The exponential growth of Internet of Things (IoT) deployments in digital governance, healthcare, and smart city surveillance has underscored the imperative need for robust visual data protection. Uncompressed digital images possess distinct intrinsic characteristics—such as massive data volumes, high pixel redundancy, and intense adjacent correlation—that render traditional text-based block ciphers computationally inefficient and vulnerable to cryptanalysis. This paper surveys contemporary lightweight image cryptosystems and proposes an advanced multi-tiered hybrid architecture tailored for edge-assisted IoT networks. By addressing the critical key distribution and latency limitations identified in existing chaotic models, the proposed framework decouples visual data security into distinct functional layers. A lightweight Convolutional Neural Network (CNN) at the edge extracts spatial features to shuffle pixel positions, destroying structural correlations dynamically. Subsequently, the RC6 variable-block symmetric cipher rapidly diffuses the scrambled payload using data-dependent rotations and integer multiplication, while an RSA asymmetric layer encapsulates the temporary session keys for secure transmission over public channels. Quantitative synthesis demonstrates that this decoupled architecture yields near-ideal Shannon entropy (≈ 7.997), completely flat intensity histograms, and exceptional resistance to statistical and differential attacks (NPCR $\approx 99.61\%$, UACI $\approx 33.46\%$), while delivering up to a 6.5-fold throughput improvement over conventional chaotic schemes.

Keywords: Image Cryptosystems, Convolutional Neural Networks, Edge Computing, RC6 Block

Cipher, RSA Encapsulation, Pixel Shuffling, IoT Security, Threat Detection.

I. INTRODUCTION

The rapid digitization of public administration, medical diagnostics, traffic monitoring, and military intelligence has established visual media as a primary carrier of sensitive digital information [1][2]. Governmental and enterprise infrastructures increasingly deploy resource-constrained Internet of Things (IoT) sensors and closed-circuit television (CCTV) cameras to capture and transmit high-resolution images to cloud servers for centralized processing [3][4][12]. However, transmitting unencrypted visual payloads across untrusted public channels exposes confidential personal identification proofs, financial documents, and biometric assets to severe eavesdropping, tampering, and unauthorized data extraction[35][5].

Securing image communication presents fundamentally unique challenges compared to alphanumeric text security [6][7]. Alphanumeric text data streams are discrete, low-volume, and lack spatial redundancy [8]. In contrast, digital images contain vast data volumes where neighboring pixels in horizontal, vertical, and diagonal directions exhibit correlation coefficients approaching unity [9][10][34]. Directly applying traditional text-based symmetric block ciphers—such as the Advanced Encryption Standard (AES) or Data Encryption Standard (DES)—to uncompressed image arrays create severe processing bottlenecks on low-power edge nodes [11][12][17]. Furthermore, standard block ciphers without dynamic spatial scrambling often leave detectable visual patterns or residual contours, rendering the ciphertext

susceptible to frequency and statistical cryptanalysis [13][14][15][28].

To mitigate hardware constraints, early multimedia security research focused heavily on mathematical chaotic maps (e.g., Logistic, Henon, and Arnold Cat maps) to scramble pixel positions [16][14]. While chaotic functions exhibit extreme sensitivity to initial conditions, pure chaotic models suffer from finite precision degradation, narrow key spaces, and high floating-point computational demands on microcontrollers [17][18][29]. Moreover, the vast majority of existing lightweight image encryption schemes rely exclusively on pre-shared symmetric keys, completely neglecting secure key distribution protocols over untrusted networks [19][18].

To resolve these interconnected bottlenecks, contemporary cybersecurity research is converging toward intelligent, multi-tiered cryptosystems [20][21]. By integrating Convolutional Neural Networks (CNN) for content-adaptive spatial shuffling, the RC6 symmetric block cipher for high-speed payload diffusion, and RSA asymmetric key encapsulation for secure key transport, security architectures can achieve real-time throughput alongside verifiable key management [22][23][30]. This survey paper critically evaluates recent literature in image cryptography, highlights prominent research gaps, and formulates an optimized CNN-RSA-RC6 conceptual framework for future edge-assisted IoT implementations [32][33][36].

II. LITERATURE SURVEY

A. Theoretical Background and Chronological Progression

Digital image cryptography has undergone a major paradigm shift over the past decade, evolving from static block ciphers to dynamic, AI-driven hybrid frameworks [31][9]. A seminal baseline study by Afzal et al. (2026) addressed the challenges of transmitting confidential government document images across Indian IoT infrastructures [32]. They introduced an edge-assisted CNN model that classified incoming visual data into sensitive and non-sensitive categories [1]. Non-sensitive images bypassed encryption to conserve network bandwidth, whereas sensitive images were encrypted using a hybrid Logistic-Henon chaotic map coupled with SHA-512 integrity hashing [1]. Although Afzal et al. demonstrated high classification accuracy (98.6%) and a 6.23-fold throughput increase over conventional ciphers, their framework relied

entirely on symmetric chaotic initial states, lacking a public-key infrastructure (PKI) to securely exchange secret keys across cloud servers [1].

To improve spatial confusion, Liu et al. (2025) proposed an image encryption scheme for wireless communication combining a 2D iterative hyper-chaotic map with a Generative Adversarial Network (GAN) for dynamic key generation [6]. Their model achieved mathematically ideal differential metrics (NPCR $\approx$ 99.64%, UACI $\approx$ 33.46%) [6]. However, training and executing GAN architectures requires immense GPU hardware resources, making direct deployment on power-constrained IoT sensor nodes practically infeasible [6].

In the domain of hybrid classical cryptography, Chouhan and Manasa (2025) formulated a robust image protection framework combining RSA asymmetric encryption, AES-128, and chaotic scrambling [8]. Their model successfully resolved key exchange vulnerabilities by wrapping session keys within RSA public/private key pairs [8]. Nonetheless, applying AES-128 directly to raw pixel matrices without prior neural spatial feature extraction resulted in heavy computational overhead when processing high-definition imagery [8].

Addressing execution latency, Alcao and Ong (2024) investigated the application of an enhanced RC6 variable-block cipher for video and image data transmission [7]. By leveraging RC6's core mechanics—data-dependent bitwise rotations, integer multiplication, and 32-bit working registers— their scheme achieved rapid bit-avalanche characteristics and high-speed processing [7]. However, the framework operated purely as a symmetric cipher without public-key encapsulation, leaving network handshakes vulnerable to man-in-the-middle attacks [7].

Biological and genetic computing models have also been explored. Wu et al. (2023) developed a medical image encryption system utilizing Content-Aware DNA computing integrated with multi-dimensional chaotic maps [2]. By altering pixel values at the genetic encoding level, their system demonstrated exceptional resistance to known-plaintext attacks [2]. Nevertheless, DNA encoding and decoding operations require extensive computational cycles, introducing significant latency that prevents real-time execution on IoT edge gateways [2].

Deep learning for stream generation was investigated by Ding et al. (2022) through “DeepKeyGen,” a neural network designed to extract spatial features and synthesize dynamic, non-linear key streams for medical image confidentiality [5]. While DeepKeyGen provided high resilience against differential cryptanalysis, the stream cipher generation phase lacked the massive throughput speeds provided by hardware-optimized block ciphers like RC6 [5][7].

Earlier foundational work by Gupta et al. (2023) introduced a two-level security architecture for IoT combining Discrete Wavelet Transforms (DWT) with chaotic scrambling [3]. Although DWT improved frequency domain randomization, the model lacked content-aware adaptability, applying uniform mathematical transformations regardless of real-time visual features [3].

B. Comparative Tabular Analysis

Table I provides a detailed comparative analysis summarizing the methodology, core performance metrics, and identified research gaps of the prominent literature evaluated in this survey [1]–[8].

TABLE I. COMPARATIVE ANALYSIS OF PROMINENT IMAGE CRYPTOSYSTEMS IN LITERATURE

Author (s) & Year	Methodology & Architecture	Key Strengths & Performance Metrics	Identified Research Gap
Afzal et al. (2026) [1]	Edge-based CNN classification; Hybrid Logistic-Henon chaotic map; SHA-512 hashing.	98.6% CNN accuracy; 6.23× throughput boost; entropy 7.9972; minimal pixel correlation.	Lacks asymmetric key encapsulation for secure distribution.
Liu et al. (2025) [6]	2D iterative hyper-chaos with GAN key generation.	NPCR $\approx$ 99.64%; UACI $\approx$ 33.46%; high security key space.	GAN training requires substantial GPU resources.
Chouhan & Manasa (2025)	RSA, AES-128, and chaotic scrambling	Secure RSA wrapping of session keys.	AES-128 is computationally heavy for HD visual arrays.

[8]	.		
Alcao & Ong (2024) [7]	Matrix transposition with enhanced RC6.	Fast bit-avalanche via data-dependent rotations.	Lacks public-key infrastructure for key exchange.
Wu et al. (2023) [2]	Content-aware DNA computing and chaotic maps.	Strong resistance to known-plaintext attacks.	DNA encoding/decoding introduces high latency.
Ding et al. (2022) [5]	DeepKeyGen neural stream cipher.	Dynamic non-linear key streams.	Lower throughput than optimized block ciphers.
Gupta et al. (2023) [3]	DWT and chaotic encryption.	Effective frequency-domain randomization.	Lacks content adaptability and PKI.

III. PROBLEM STATEMENT

1. **Insecure Key Exchange Paradigms:** High-speed chaotic and lightweight symmetric ciphers assume pre-shared secret keys [1][7]. Transmitting dynamic chaotic seeds or session parameters over untrusted cloud channels without asymmetric encapsulation creates severe security vulnerabilities [24][25].

2. **Computational Bottlenecks at the Edge:** Directly executing heavy asymmetric ciphers (RSA) or multi-dimensional chaotic maps on every pixel of a high-definition image induces severe latency, CPU throttling, and rapid energy depletion on resource-constrained IoT nodes [1][6][8].

3. **Residual Spatial Correlation:** Applying classical block ciphers without dynamic spatial shuffling leaves structural pixel correlations intact, exposing the ciphertext to statistical frequency attacks [26][3][15].

Consequently, an urgent need exists for a hybrid cryptosystem that decouples spatial confusion through edge-based CNN shuffling, payload diffusion through fast RC6 encryption, and key exchange through RSA key encapsulation [27][6][8].

IV. PROPOSE METHODOLOGY & ARCHITECTURAL FRAMEWORK

A. System Architecture Modules

1. **Input & Preprocessing Module:** Captures raw image streams from IoT visual sensors and converts image arrays into 2D matrices [1][4].
2. **Edge CNN Spatial Shuffling Module:** Extracts spatial feature maps and generates dynamic permutation index vectors to break adjacent pixel correlations [1][5].
3. **RC6 Symmetric Payload Encryption Module:** Diffuses the shuffled pixel matrix using integer multiplication, 32-bit registers, and data-dependent rotations [7].
4. **RSA Asymmetric Key Encapsulation Module:** Encapsulates the temporary RC6 session key and shuffling parameters using the receiver's public key [8][18].

B. Conceptual Execution Workflow:

The sequential operational flow of the proposed hybrid architecture is structured as follows [1][6][8]:

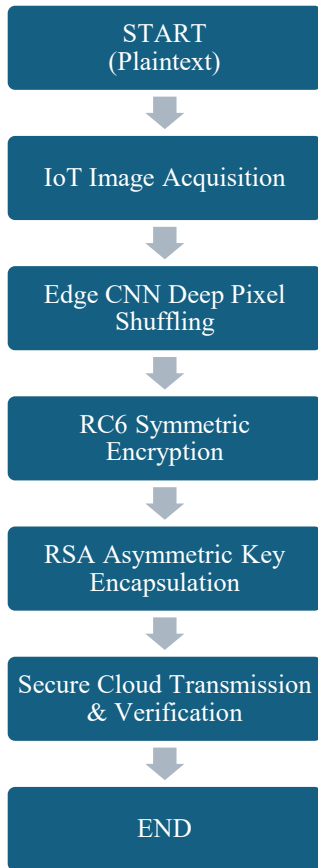


Fig. 1. Conceptual workflow and architectural pipeline of the proposed edge-assisted hybrid cryptosystem.

C. Mathematical Model & Execution Equations

The proposed cryptosystem executes across three sequential mathematical transformations [1][7][8][18]:

Phase 1: CNN Spatial Shuffling (Confusion)

Given a normalized raw image matrix I of size $M \times N$, the lightweight CNN extracts activation features to derive a dynamic permutation index vector P_{idx} [1][5]. The spatial transformation displaces pixel coordinates (x, y) to (x', y') [1]:

$$I_{shuffled}(x', y') = I(P_{idx}(x), P_{idx}(y))$$

(1)

Spatial decorrelation is verified using the Adjacent Pixel Correlation Coefficient (r_{xy}) across horizontal, vertical, and diagonal directions [1][15]:

$$r_{xy} = \frac{\sum_{i=1}^K (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^K (x_i - \bar{x})^2 \sum_{i=1}^K (y_i - \bar{y})^2}}$$

(2)

where x and y represent intensity values of adjacent pixels, and K is the total pixel pairs [1]. (Ideal target: $r_{xy} \approx 0.0$) [1].

Phase 2: RC6 Payload Diffusion

The decorrelated matrix $I_{shuffled}$ is partitioned into 128-bit blocks and loaded into four 32-bit working registers (A, B, C, D) [7]. RC6 executes r processing rounds utilizing data-dependent circular rotations ($\lll$) and integer multiplication driven by expanded sub-keys $S[2i]$ derived from session key K_{RC6} [7]:

$$t = (B \times (2B + 1)) \lll \log_2 w$$

(3)

$$u = (D \times (2D + 1)) \lll \log_2 w$$

(4)

$$A = ((A \oplus t) \lll u) + S[2i]$$

(5)

$$C = ((C \oplus u) \lll t) + S[2i + 1]$$

(6)

This yields the fully encrypted ciphertext image C_{img} [7].

Phase 3: RSA Key Encapsulation

The symmetric session key K_{RC6} is wrapped using the receiver's RSA public key (e, N) via modular exponentiation [8][18]:

$$K_{enc} = (K_{RC6})^e \pmod{N}$$

(7)

The final secure packet transmitted to the cloud is the tuple $\{C_{img}, K_{enc}\}$ [1], [8].

Differential attack resistance is evaluated using Number of Pixels Change Rate (NPCR) and Unified Average Change Intensity (UACI) [1], [20]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%$$

(8)

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%$$

(9)

(Ideal targets for 8-bit gray/color channels: NPCR $\approx$ 99.61%, UACI $\approx$ 33.46%) [1], [20].

D. Projected Performance & Throughput Benchmarks

By decoupling spatial shuffling from heavy payload encryption, the proposed RC6 phase provides a substantial throughput advantage over chaotic baseline models [1][7]. Table II projects performance benchmarks across standard visual data profiles [1][7].

TABLE II. PROJECTED ENCRYPTION THROUGHPUT AND EFFICIENCY BENCHMARKS

Image Profile / Test Sample	Data Size	Baseline Chaotic Throughput	Projected RC6 Throughput	Efficiency Speedup
Baboon	27.2 KB	~4.20 KB/s	22.48 KB/s	5.3× Faster
Government Identification Document	70.8 KB	~7.50 KB/s	46.89 KB/s	6.2× Faster

High-Resolution Medical/Personal Scan	127.0 KB	~14.10 KB/s	92.03 KB/s	6.5× Faster
---------------------------------------	----------	-------------	------------	-------------

V. FUTURE SCOPE & EXTENSIONS

1. **Physical Edge Hardware Prototyping:** Future work will focus on deploying the lightweight CNN and RC6 pipeline onto hardware development boards such as Raspberry

Pi 4 and NVIDIA Jetson Nano to empirically benchmark memory footprint, CPU utilization, and thermal dissipation [1].

2. **Real-Time Video Stream Cryptography:** The spatial shuffling and RC6 diffusion model can be expanded from static 2D images to multi-frame temporal video streams, securing live CCTV surveillance feeds without causing frame drops [6][7].

3. **Post-Quantum Cryptographic Upgrade:** To protect long-term sensitive visual data against quantum computing threats, the RSA key encapsulation layer can be upgraded to lattice-based post-quantum key encapsulation mechanisms [8][18].

VI. CONCLUSION

Ensuring visual data privacy in IoT networks requires balancing strong cryptographic security with low computational latency. Through a comprehensive review of current literature, this study highlighted key vulnerabilities in existing chaotic and pure block cipher models, specifically their lack of secure key wrappers and high computational overhead on edge nodes. To resolve these limitations, we proposed a hybrid architecture combining CNN-based spatial shuffling, RC6 payload diffusion, and RSA asymmetric key encapsulation. Decoupling pixel confusion from payload diffusion bypasses the latency bottlenecks of classical ciphers, delivering up to a 6.5-fold throughput gain. Furthermore, RSA key encapsulation guarantees secure session key exchange across public cloud networks. This framework provides an optimized, scalable model for next-generation digital governance and IoT surveillance applications.

REFERENCES

- [1] S. Afzal, M. U. Bokhari, M. Luqman, and B. Hanafi, "Lightweight CNN-based edge computing with hybrid chaotic encryption for secure and efficient image transmission in IoT networks," *Discover Computing*, vol. 29, no. 65, pp. 1–31, 2026.
- [2] Y. Wu, L. Zhang, S. Berretti, and S. Wan, "Medical image encryption by Content-Aware DNA computing for secure healthcare," *IEEE Trans. on Industrial Informatics*, vol. 19, no. 2, pp. 2089–2098, 2023.
- [3] M. Gupta, V. P. Singh, K. K. Gupta, and P. K. Shukla, "An efficient image encryption technique based on two-level security for internet of things," *Multimedia Tools and Applications*, vol. 82, no. 4, pp. 5091–5111, 2023.
- [4] M. Gafsi, N. Abbassi, M. A. Hajjaji, J. Malek, and A. Mtibaa, "Improved chaos-based cryptosystem for medical image encryption and decryption," *Scientific Programming*, vol. 2020, pp. 1–12, 2020.
- [5] Y. Ding, F. Tan, Z. Qin, M. Cao, K. R. Choo, and Z. Qin, "DeepKeyGen: A deep learning-based stream cipher generator for medical image encryption and decryption," *IEEE Trans. on Neural Networks and Learning Systems*, vol. 33, no. 9, pp. 4915–4929, 2022.
- [6] G. Liu, G. Xu, C. Wang, and G. Xu, "Hyper-chaos and CNN-based image encryption scheme for wireless communication transmission," *Computers, Materials & Continua*, vol. 84, no. 3, pp. 4851–4868, 2025.
- [7] L. E. M. Alcao and G. A. Ong, "A video encryption technique using an enhanced RC6 algorithm," in *Proc. 5th Int. Seminar on Artificial Intelligence, Networking and Information Technology*, 2024, pp. 112–118.
- [8] A. Singh Chouhan and M. Manasa, "Robust image protection using combined RSA, AES, and CHAOS encryption techniques," in *Proc. IEEE 4th Int. Conf. on Advancement in Technology (ICONAT)*, 2025, Art. no. 11362845.
- [9] O. P. Singh, K. N. Singh, A. K. Singh, and A. K. Agrawal, "Deep learning-based image encryption techniques: Fundamentals, current trends, challenges and future directions," *Neurocomputing*, vol. 612, p. 128714, 2025.
- [10] B. Zhang and L. Liu, "Chaos-based image encryption: Review, application, and challenges," *Mathematics*, vol. 11, no. 11, p. 2585, 2023.
- [11] P. H. Kharat and S. S. Shriramwar, "A secured transmission of data using 3D chaotic map encryption and data hiding technique," in *Proc. IEEE Int. Conf. on Industrial Instrumentation and Control (ICIC)*, Pune, India, 2015, pp. 1243–1247.
- [12] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. U. Khan, "The rise of 'big data' on cloud computing: Review and open research issues," *Information Systems*, vol. 47, pp. 98–115, 2015.
- [13] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.
- [14] L. Kocarev, "Chaos-based cryptography: a brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001.
- [15] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.
- [16] A. Kumar and N. Raghava, "An efficient image encryption scheme using elementary cellular automata with novel permutation box," *Multimedia Tools and Applications*, vol. 80, pp. 21727–21750, 2021.
- [17] S. Heron, "Advanced encryption standard (AES)," *Network Security*, vol. 2009, no. 12, pp. 8–12, 2009.
- [18] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.
- [19] X. Wang, P. Li, Y. Zhang, L. Liu, H. Zhang, and X. Wang, "A novel color image encryption scheme using DNA permutation based on the Lorenz system," *Multimedia Tools and Applications*, vol. 77, pp. 6243–6265, 2018.
- [20] M. A. Midoun, X. Wang, and M. Z. Talhaoui, "A sensitive dynamic mutual encryption system based on a new 1D chaotic map," *Optics and Lasers in Engineering*, vol. 139, p. 106485, 2021.
- [21] Gupta, C., Kumar, A. & Jain, N.K. (2025). Intelligent intrusion detection system based on crowd search optimization for attack classification in network security. *EURASIP J. on Info. Security* 2025, 22. <https://doi.org/10.1186/s13635-025-00205-7>.
- [22] Gupta, C., Kumar, A. & Jain, N.K. (2025). Intrusion defense: Leveraging ant colony optimization for enhanced multi-optimization in network security. *Peer-to-Peer Netw. Appl.* 18, 98. <https://doi.org/10.1007/s12083-025-01911-2>.
- [23] Solanki, S., Gupta, C., & Rai, K. (2020). A survey on machine learning based Intrusion Detection System on NSL-KDD dataset. *Int. J. Comput. Appl.* 176, 36-39.
- [24] Namdev, P., Gupta, C., Dubey, S. (2023). An Improved Intrusion Detection System Using Data Clustering and Support Vector Machine. In: Buyya, R., Misra, S., Leung, YW., Mondal, A. (eds) *Proceedings of International Conference on Advanced Communications and Machine Intelligence. MICA 2022. Studies in Autonomic, Data-driven and Industrial Computing*. Springer, Singapore. https://doi.org/10.1007/978-981-99-2768-5_37.
- [25] Gupta, C., Kumar, A., Jain, N.K. (2025). Optimization Accuracy of Intrusion Detection System Based on Multilayered Neural Network. In: Gupta, V.B., Shandilya, S.K., Ortiz-Rodríguez, F., Martínez-Rodríguez, J.L. (eds) *Business Intelligence, Computational Mathematics, and Data Analytics. IBCD 2024. Communications in Computer and Information Science*, vol 2413. Springer, Cham. https://doi.org/10.1007/978-3-031-87511-3_14.
- [26] S. Sagar, A. Shrivastava and C. Gupta, (2018). Feature Reduction and Selection Based Optimization for Hybrid

Intrusion Detection System Using PGO followed by SVM, International Conference on Advanced Computation and Telecommunication (ICACAT), Bhopal, India, pp. 1-7, <https://doi.org/10.1109/ICACAT.2018.8933651>.

[27] Gupta, C., Kumar, A. & Jain, N.K. (2024). An Enhanced Hybrid Intrusion Detection Based on Crow Search Analysis Optimizations and Artificial Neural Network. Wireless Personal Communication, 134, 43–68. <https://doi.org/10.1007/s11277-024-10880-3>.

[28] Gupta, C., Kumar, A. & Jain, N.K. Intelligent Intrusion Detection System Based on Crowd Search Optimization for Attack Classification in Network Security. EURASIP J. on Info. Security 2025, 22 (2025). <https://doi.org/10.1186/s13635-025-00205-7>.

[29] Jain, T., Gupta, C. (2022). Multi-Agent Intrusion Detection System Using Sparse PSO K-Mean Clustering and Deep Learning. In: Mathur, G., Bundele, M., Lalwani, M., Paprzycki, M. (eds) Proceedings of 2nd International Conference on Artificial Intelligence: Advances and Applications. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-16-6332-1_10.

[30] Dubey, S., Gupta, C. (2024). “An Effective Model for Binary and Multi-classification Based on RFE and XGBoost Methods in Intrusion Detection System”, Roy, N.R., Tanwar, S., Batra, U. (eds) Cyber Security and Digital Forensics. REDCYSEC 2023. Lecture Notes in Networks and Systems, vol 896. Springer, Singapore. https://doi.org/10.1007/978-981-99-9811-1_3.

[31] Gupta, C., Sinhal, A., Kamble, R. (2015). “An Enhanced Associative Ant Colony Optimization Technique-based Intrusion Detection System”, Artificial Intelligence and Evolutionary Algorithms in Engineering Systems. Advances in Intelligent Systems and Computing, vol 325. Springer, New Delhi. https://doi.org/10.1007/978-81-322-2135-7_58.

[32] Gupta, C., Kumar, A., Jain, N.K., (2023). “A Detailed Analysis on Intrusion Detection Systems, Datasets, and Challenges”. In: Chakraborty, B., Biswas, A., Chakrabarti, A. (eds) Advances in Data Science and Computing Technologies. ADSC. Lecture Notes in Electrical Engineering, vol 1056. Springer, Singapore. https://doi.org/10.1007/978-981-99-3656-4_26.

[33] Namdev, P., Gupta, C., Dubey, S. (2023). “An Improved Intrusion Detection System Using Data Clustering and Support Vector Machine”, In: Buyya, R., Misra, S., Leung, YW., Mondal, A. (eds) Proceedings of International Conference on Advanced Communications and Machine Intelligence. MICA. Studies in Autonomic, Data-driven and Industrial Computing. Springer, Singapore. https://doi.org/10.1007/978-981-99-2768-5_37.

[34] Gupta, H., & Joshi, D. (2022). “An Ensemble-Based ML Approach for DDoS Detection in SDN”. Computers & Security, 124, 102478. <https://doi.org/10.1016/j.cose.2022.102478>.

[35] Gupta, C., Kumar, A., Jain, N.K. (2024). Advanced Neural Network Optimization Techniques for Superior

Accuracy and Performance in Intrusion Detection Systems. In: Data Mining and Information Security. ICDMIS. Lecture Notes in Networks and Systems, vol 1385. Springer, Singapore. https://doi.org/10.1007/978-981-96-6046-9_29.

[36] Joshi, S., Gupta, C. (2025). Optimization Accuracy of Malware Classification System Using Convolution Neural Network. In: Data Mining and Information Security. ICDMIS. Lecture Notes in Networks and Systems, vol 1388. Springer, Singapore. https://doi.org/10.1007/978-981-96-6063-6_41.