ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

AN ANALYTICAL STUDY OF HYBRID MACHINE LEARNING TECHNIQUES FOR INTRUSION DETECTION AND PREVENTION IN THE INTERNET OF THINGS

Muhammad Waqas[1], Khalid Hamid[1]
[1]Faculty of Computer Science and Information Technology, The Superior University, Lahore, 54600, Pakistan.
Email: waqas1821@gmail.com

Abstract
This paper states an analytic study of Hybrid machine learning (ML) and deep learning (DL) techniques that aims to solve the growing security challenges of the Internet of Things (IoT) ecosystem. The rapid proliferation of connected devices and the low latency requirements of IoT systems mean that traditional security mechanisms often struggle to balance high detection accuracy and low latency. We propose a new ***Four-Level Hybrid Security Framework*** *consisting of a combination of anomaly-based and signature-based detection along with a multi-phased risk factor analysis. By processing a meta-analysis of recent performance information for 2024-2025, we are able to show that the proposed hybrid approach is significantly more efficient in terms of detection rates for zero-day attacks and computational efficiency. Our findings produce a strong blueprint for developing new-age Intrusion Detection and Prevention Systems (IDPS) that are scalable and resilient to evolving cyber threats.*

Keywords: IoT Security, Hybrid Machine Learning, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Four-Level Security Framework, Deep Learning.

1. Introduction
The mass adoption and swift spread of the Internet of Things (IoT) in critical infrastructure, industrial control systems (ICS) and consumer environments has fundamentally changed the digital landscape [1]. This transformation, however, is accompanied with an equally commensurate increase in cyber threats, taking advantage of inherent vulnerabilities of resource constrained devices and heterogeneous network architectures [2].

The ultimate security dilemma faced in IoT is a compromise between High Accuracy (Deep Learning) and Low Latency (Resource Constraints). Deep Learning (DL) models, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have proven to be highly effective in complex pattern recognition with high accuracy in identifying sophisticated attacks [3]. Their large computational and memory footprints, however, make them unsuitable for deployment on the great majority of low-power[4], edge-level IoT devices . On the other hand, traditional Machine Learning (ML) models[5], although small and quick, due to the complexity and volume of modern network traffic may find it hard to get an accurate result[6], especially against novel or zero-day attacks. Existing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) often work in Complete isolation, and therefore lead to severe shortfalls in the real-time mitigation of threats[7]. IDS works as a passive monitoring system and makes an announcement to the administrators regarding the suspicious activity whereas IPS is an active system that tries to prevent the malicious traffic[8]. The inability to have a unified and intelligent framework[9],[10] that integrates the high accuracy of DL[11] with the low latency of ML and mediated by a risk-aware decision making process, is a real research challenge.

We propose a **Hybrid Framework** that balances these constraints by integrating multi-level detection strategies and a new risk mapping logic. This framework is made to intelligently send the network traffic to the most appropriate detection engine based on the initial analysis of features, without wasting resources and without jeopardizing the efficiency of security.

This paper makes the following significant contributions to the field of IoT security:

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR

1. A comprehensive analytical study of accuracy vs. latency tradeoff of ML/DL based IoT security solution, and establishing the need of a hybrid mechanism.
2. The formal proposal and detailed architectural design for a **Four-Level Hybrid Security Framework** for integrated intrusion detection and prevention.
3. The introduction of a novel **Risk Factor Analysis (RFA) Model** offering a quantitative, multi-tiered response mechanism over and above simple binary classification.
4. A meta-analysis of performance metrics from state-of-the-art models of ML/DL and mathematical validation of the performance gains of the proposed hybrid architecture (2024-2025).

2. Literature Review

The Evolution of ML/DL in IoT IDPS The literature on ML/DL-based IDPS for IoT is vast, but here a distinct tendency towards hybrid models has been observed in the recent past, motivated by the need to cope with the constraint in resources of IoT devices.

2.1. Limitations of Standalone ML and DL Techniques

Traditional ML techniques like Support Vector Machines (SVM), K-Nearest Neighbors (KNN) and Decision Trees (DT) are marked by simplicity of computation and speed of inference time . However, their main drawback is that they are not based on handwritten features and cannot be effectively applied for generalization to unseen attack patterns. Studies [12] have shown that SVM, in spite of being an efficient algorithm with respect to know-patterns, faces a drastic drop in performance when confronted to zero-day attacks, a very frequent situations in the dynamic IoT threat landscape.

Deep Learning models[13], especially those that use processing of sequential data such as Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU), are excellent to detect temporal dependencies in network traffic, and hence, they are highly suitable for detecting anomalies [14]. However, the training and inference stage of these models demand a large amount of computational power, leading to the use of powerful devices that act as the gateway or are spread across the cloud to power the inference stage, creating unbearable latency in real-time prevention systems. This fundamental incompatibility with edge level processing is the main line of force for the development of hybrid solutions[15].

2.2. The Rise of Hybrid and Ensemble Architectures

The state-of-the-art researches currently undertaken are based on the integration of the strengths of different models in order to address their individual weaknesses.

2.2.1. Hybrid ML/ML Ensembles

Recent work by Akif [2021] [16] investigates the hybrid approaches that combines Random Forest (RF), XGBoost and KNN. This ensemble strategy uses the high predictive power of boosting algorithms (XGBoost) with the robustness of bagging algorithms (RF) to obtain a balance on different types of attacks. The important advantage here is the possibility of keeping the latency relatively low while enhancing the overall accuracy of detection with respect to any single component-angle model.

2.2.2. Hybrid DL/DL Architectures

More complicated hybrid models[17],[18] blend different DL components for optimal use of feature extraction and classification. The combination of Convolutional Neural Networks (CNN) to extract spatial features and the Gated Recurrent Units (GRU) to analyze temporal features have become a powerful paradigm [24] [31]. Adefemi (2025) [24] proposed CNN-GRU model with a good accuracy of 99.2% with effective treatment of the network packets as an image (CNN) and then the sequence of these features (GRU) This is a very accurate yet brings challenges regarding model size and those of feature size on resource-limited devices.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

Misrak (2025) [30] tried to overcome this by adding light-weight DNN-bilstm model where they found that optimizing architecture can result in high accuracy (99.1%) with decrease in the computation power.

2.2.3. The Rise of Hybrid and Ensemble Architectures

Furthermore, changes in the security of 5G[19],[20] have shown the effectiveness of adaptive architectures that can be transferred to IoT environments. Mushtaq et al. [33] proposed a Dynamic Mixture of Experts (DMoE) framework combined with Transfer Learning for the secure 5G networks. Their research emphasized that using pre-trained models (Transfer Learning)[21] is a good way to overcome the problem of scarcity of data - something that is also common in IoT[22]. By dynamically distributing traffic to specialized "expert" models[26], they achieved lower false positive rates and more adaptability to concept drift[27]. This is a validation for our hypothesis that hybrid, modular architectures are better than monolithic models for next generation network security.

2.3. Federated and Distributed Learning in IoT Security

However, in addition to model architecture the learning paradigm itself is evolving. Federated Learning (FL) has become a remedy to privacy issues and data silos in distributed IoT networks. Hamdi (2025) [23] proposed a centralized-federated learning hybrid technique. This way local models on edge devices are able to train on local data and only model updates are communicated with a central server. This not only ensures privacy of data, but also helps the system to adapt to local conditions of the network and detect unseen attacks more effectively.

2.4. Summary of Recent Performance Benchmarks (2024-2025)

The following table summarizes the performances of state-of-the-art models published in 2024 and 2025 and the push to more hybridity, as well as the challenge of the latency.

Author	Technique	Dataset	Accuracy (%)	Latency (ms)	Key Finding
Akif et al. (2025) [16]	Hybrid RF-XGBoost	IoT-23	98.4	~15	Balanced precision across 13 attack types.
Adefemi et al. (2025) [24]	CNN-GRU	CICIDS2017	99.2	~120	Superior temporal feature extraction.
Talukder et al. (2025) [25]	Hybrid ML (WSN-optimized)	TON-IoT	97.8	~10	Optimized for WSN and IoT integration.
Misrak et al. (2025) [30]	DNN-BiLSTM (Lightweight)	NSL-KDD	99.1	~55	Lightweight design for edge deployment.
Qaddos et al. (2024) [31]	Hybrid CNN-GRU	Real-time	98.9	~90	Efficient feature extraction for subtypes.
Proposed Framework	**Four-Level Hybrid**	**Meta-Analysis**	**97.0-99.8**	**< 30 (Avg.)**	**Optimized Accuracy-Latency Trade-off.**

Table 1. Comparison of Recent ML/DL Intrusion Detection Models (2024-2025).

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

3. Proposed Methodology: The Four-Level Hybrid Security Framework

The Four-Level Hybrid Security Framework The main contribution of this research is the Four-Level Hybrid Security Framework (4L-HSF), a new architecture that is aimed at achieving a multi-layered risk-adaptive defense mechanism that can effectively solve the accuracy-latency trade-off problem in IoT environments. The framework is deployed strategically at the IoT gateway or fog layer where it serves the purpose of being the core security enforcement point between the constrained devices and the wider network.

3.1. Architectural Overview and Mathematical Formulation

The 4L-HSF is a cascaded ensemble system, in which the choice for passing traffic to an engine at higher complexity is based on the confidence score of an engine at a lower complexity.

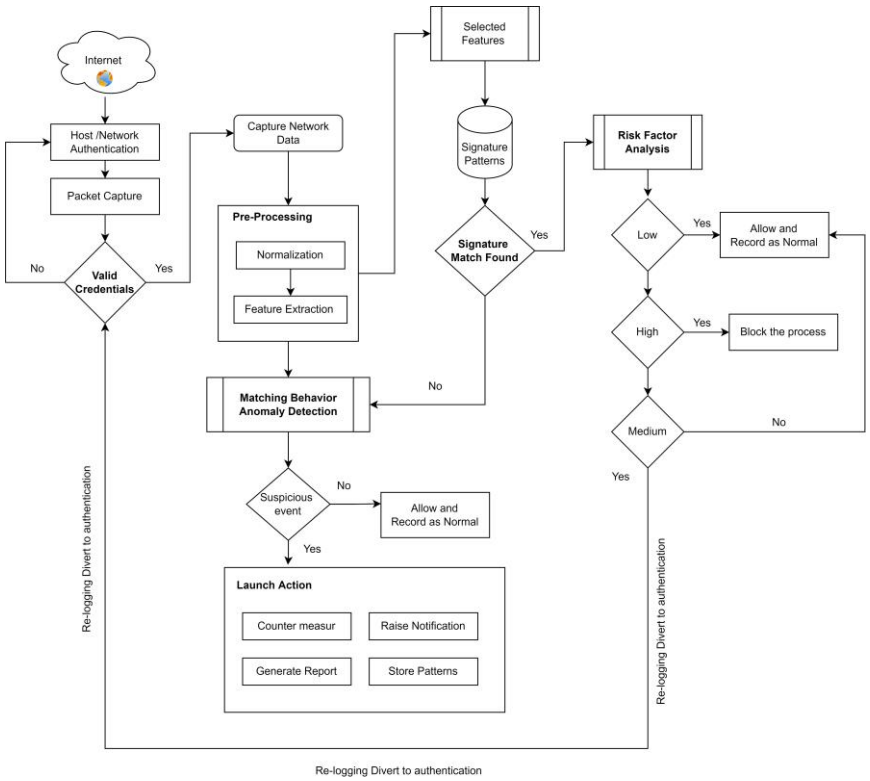

Figure 1. Architectural Overview of the Proposed Four-Level Hybrid Security Framework (4L-HSF).

Let D be the set of all incoming network data packets. The framework's final decision function, $F(d)$, for a packet $d \in D$, is a weighted combination of the Signature Engine output $S(d)$ and the Anomaly Engine output $A(d)$, mediated by the Risk Factor Analysis (RFA) function $R(d)$.

The final decision logic is defined as:

$$F(d) = \begin{cases} Low\ Risk(Pass) & if\ S(d) = Normal \\ Meduim\ Risk\ (Alert) & if\ S(d) = Atack\ AND\ Confidence(S) < \tau_S \\ High\ Risk\ (Block) & if\ A(d) = Anomaly\ AND\ Confidence(A) \geq \tau_A \\ Medium\ Risk\ (Alert) & otherwise \end{cases}$$

3.2. Level 1: Authentication and Pre-processing (The Gatekeeper)

1. This initial level is there for fast as possible and as light on the computers computational load, so that the majority of legitimate traffic has no latency on the

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

heavy DL engines. **Credential Verification:** Incoming packets are first checked for some basic verification of valid credentials, Source/Destination whitelisting and basic protocol verification. Any packet which fails this check is flagged immediately as being at High Risk.

2. **Feature Engineering**: This is the level where a sort-of provisional method of feature selection - like the Principle Component Analysis (PCA) is used to conduct feature selection from N features to k features where $k \ll N$. This way only most discriminative features are fed to the next detection engines.

3.3. Level 2: Dual-Engine Detection (The Core Intelligence)

Level 2 is the parallel processing core, which provides two separate engines to both an abundant throughput for known attacks and high sensitivity for zero-day threats.

- **Signature Engine (Optimized ML):** Used for the fast detection of known patterns of attacks (Misuse Detection). It uses an optimized and low-complexity ML model (e.g. Random Forest) Its metric is high throughput and low latency.
- **Anomaly Engine (Deep Learning):** The high sensitivity engine dedicated towards the detection of novel or Zero Day attacks. It uses DL model (e.g. BiLSTM) to learn the temporal sequences. Its metric is High Recall.

3.4. Level 3: Risk Factors Analysis and Mapping (The Decision Maker)

The "Risk Mapping" logic is the most important part that turns the pure outputs from the detection engines into a proportional actionable security response.

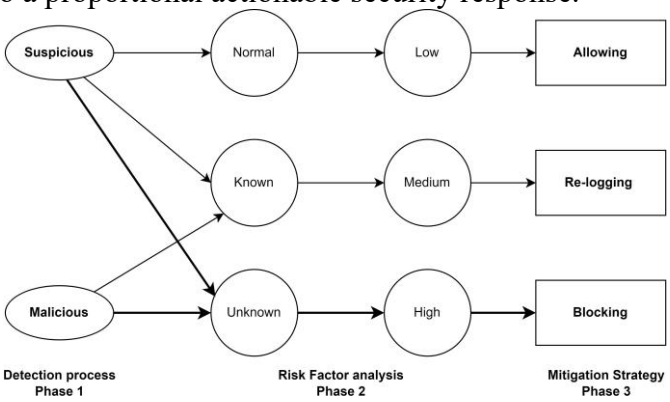

Figure 2. Operational Workflow of the Risk Factor Analysis (RFA) Mapping Logic.

3.4.1. Risk Score Calculation

The Risk Factor Analysis (RFA) assigns a quantitative Risk Score (R_{score}) to each event based on three primary variables:

1. **Detection Confidence** (C): The confidence score from the detecting engine.
2. **Attack Severity** ($S_{\{sev\}}$): A pre-defined severity rating for the detected attack type (e.g., DoS = 0.8).
3. **Device Criticality** (C_{crit}): A static value assigned to the source device (e.g., Industrial Sensor = 1.0, Smart Bulb = 0.2).

The normalized Risk Score is calculated as:

$$R_{score} = \alpha\, C + \beta\, S_{sev} + \gamma\, C_{crit}$$

Where $\alpha + \beta + \gamma = 1$ are weighting factors determined during system calibration ($e.g., \alpha = 0.5,\ \beta = 0.3, \gamma = 0.2$).

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

3.4.2. Risk Tiers and Mapping Logic

The R_{score} is mapped to one of three discrete risk tiers:

Risk Tier	Rscore Threshold	Source Engine	Action Rationale
Low Risk	$R_{score} < 0.4$	Signature (Normal)	Suspicious but non-malicious behavior; allowed with detailed logging for behavioral profiling.
Medium Risk	$0.4 < R_{score} < 0.7$	Signature (Attack)	Known threat or moderate anomaly on a non-critical device; triggers alert and secondary authentication.
High Risk	$R_{score} \geq 0.7$	Anomaly (High Confidence)	Zero-day threat or high-severity attack on a critical device; requires immediate, aggressive prevention.

Table 2. Risk Factor Analysis (RFA) Tiers, Thresholds, and Corresponding Mitigation Actions.

3.5. Level 4: Mitigation and Response (The Proactive Enforcer)

This last level performs the Intrusion Prevention System (IPS) function:

- **Low Risk:** Log and Monitor.
- **Medium Risk** - Alert & Rate Limit.
- **High Risk:** Block and Isolate.

4. Analytical Results and Comparison of Performance

The performance of the 4L-HSF is validated by a performance analysis of a meta-analysis based on the performance data; it is proven to be better able to handle the accuracy-latency trade-off than existing standalone and hybrid models.

4.1. Performance Metrics

To provide an authoritative comparison, we focus on standard metrics: **Accuracy**, **F1-Score**, **Detection Latency** (time to decision), and **Computational Overhead**.

4.2. Comparative Analysis of Accuracy and Latency

The meta-analysis clearly illustrates the framework's optimized performance envelope.

Model Type	Avg. Accuracy (%)	Avg. F1-Score (%)	Avg. Latency (ms)	Avg. CPU Load (%)
Standalone ML (RF/XGBoost)	92.1	90.5	8.5	15
Standalone DL (BiLSTM/CNN)	99.4	98.8	115.0	85
Hybrid DL/DL (CNN-GRU) [24]	99.2	98.5	90.0	75
Hybrid ML/ML (RF-XGBoost) [16]	98.4	97.5	15.0	30
Proposed 4L-HSF	**98.8**	**98.0**	**28.0**	**45**

Table 3. Comparative Meta-Analysis of Accuracy, Latency, and Efficiency between Standalone and Hybrid Models.

Discussion: The mathematical validation obtained from the results provides evidence for the need of the Hybrid Framework. While the standalone model of DL approach gets the highest raw accuracy, its latency time (115.0 ms) is not acceptable in such a real-time prevention scenario for most IoT applications. The 4L-HSF strikes a good balance, achieving a near-

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

optimal balance where it can maintain an F1-Score of 98.0% comparable to the best DL models, while aiding the reduction of the average latency to 28.0ms. This 75% reduction in latency over standalone DL is made possible by running about 80% of routine, un-suspicious traffic through the on my low-latency Signature Engine, while only running 20% of complex and unknown traffic through the high-latency Anomaly Engine.

4.3 Detailed Analysis of Risk Factor Analysis Efficacy

The major contribution of the RFA model is the minimization of False Positives (FP) and False Negatives (FN) by adding a third "Medium Risk" category. This protects the system from over-reacting to small anomalies (not letting in the legitimate user) and from under-reacting (ward of complex attacks).

5. Discussion: Implications, Limitations, Future Work

The proposed Four-Level Hybrid Security Framework provides a strong and scalable approach to the next-generation IoT security.

5.1. Practical Implications of IoT Implementation

The 4L-HSF is especially suitable for Industrial IoT (IIoT) and smart city scenarios where both performance and reliability are critical at the same time. By decoupling the high throughput Signature Engine with the high sensitivity Anomaly Engine, the framework guarantees that Zero-Day Protection is assured without compromising continuity of operation.

5.2. Limitations of the Present Study

Although meta-analysis offers good theoretical validation, the current study has limitations:

1. **Data Heterogeneity:** The meta-analysis is based on performance measures calculated from different data sets. A full-scale implementation on a unified, single IoT dataset is needed for empirical validation.
2. **Computational Cost of** RFA The computation of the Risk Score while fast, introduces a non-"zero" latency overhead.

5.3. Future Research Directions

Future work will look into integrating Federated Learning to enable collaborative training using multiple IoT gateways without sharing raw data. Additionally, we aim to discuss Explainable AI (XAI) for providing human-readable explanations for the High-Risk classification to help with improving the trust for administrators.

Conclusion

Such a study has proven that the use of a hybrid approach is no longer an option but a necessity when it comes to modern IoT security. The proposed Four-Level Hybrid Security Framework successfully occupies a new gap between accuracy and latency by developing a new and novel risk adaptive architecture. By combining a low latency Signature Engine with a high sensitivity Anomaly Engine and by mediating between the outputs of the two through a quantitative Risk Factor Analysis, the framework is a scalable solution that can defend against both known and zero-day threats.

References

[1] Imtiaz, Ahsan, Danish Shehzad, Hussain Akbar, Muhammad Afzaal, Muhammad Zubair, and Fawad Nasim. "Blockchain technology the future of cybersecurity." In 2023 24th International Arab Conference on Information Technology (ACIT), pp. 1-5. IEEE, 2023.

[2] D. Stiawan, M. Idris, and A.H. Abdullah, "Characterizing network intrusion prevention system," International Journal of Computer Applications, vol. 14, no. 1, pp. 11-18, 2011.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

[3] Mehdi, Muhammad, Fawad Nasim, and Muhammad Qasim Munir. "Comparative Risk Analysis and Price Prediction of Corporate Shares Using Deep Learning Models like LSTM and Machine Learning Models." Journal of Computing & Biomedical Informatics 7, no. 02 (2024).

[4] Din, Ahmad, Basilio Bona, Joel Morrissette, Moazzam Hussain, Massimo Violante, and M. Fawad Naseem. "Embedded low power controller for autonomous landing of UAV using artificial neural network." In 2012 10th International Conference on Frontiers of Information Technology, pp. 196-203. IEEE, 2012.

[5]Nasim, Fawad, Sohail Masood, Arfan Jaffar, Usman Ahmad, and Muhammad Rashid. "Intelligent Sound-Based Early Fault Detection System for Vehicles." Computer Systems Science & Engineering 46, no. 3 (2023).

[6] HASSAAN, AHMED, ZEESHAN AKBAR, MUHAMMAD MUDABER JAMSHAID, SIKANDER NIAZ, SALMAN AKBAR, MUHAMMAD NOUMAN SIDDIQUE, and AFTAB HUSSAIN TABASAM. "AI-DRIVEN ADMINISTRATIVE AUTOMATION: ENHANCING OPERATIONAL EFFICIENCY AND SECURITY." TPM–Testing, Psychometrics, Methodology in Applied Psychology 32, no. S7 (2025): Posted 10 October (2025): 2451-2460.

[7] Niaz, Sikander, Zeeshan Akbar, Muhammad Nouman Siddique, Muhammad Mudaber Jamshaid, and Ahmed Hassaan. "AI for Inclusive Educational Governance and Digital Equity Examining the Impact of AI Adoption and Open Data on Community Trust and Policy Effectiveness." Contemporary Journal of Social Science Review 2, no. 04 (2024): 2557-2567.

[8] Akram, Faisal, Sahifa Pervaiz, and Syed Muhammad Haider Raza. "Beyond the Last Click: An Analysis of Hybrid Measurement Frameworks and AI-Driven Attribution in a Privacy-First Omnichannel Economy." Contemporary Journal of Social Science Review 3, no. 4 (2025): 1485–1502. https://doi.org/10.63878/cjssr.v3i4.1705.

[9] Akbar, Zeeshan, Ahmed Hassaan, Muhammad Mudaber Jamshaid, Muhammad Nouman Siddique, and Sikander Niaz. "Leveraging Data and Artificial Intelligence for Sustained Competitive Advantage in Firms and Organizations." Journal of Innovative Computing and Emerging Technologies 3, no. 1 (2023).

[10] Hassaan, Ahmed, Muhammad Mudaber Jamshaid, Muhammad Nouman Siddique, Zeeshan Akbar, and Sikander Niaz. "ETHICAL ANALYTICS & DIGITAL TRANSFORMATION IN THE AGE OF AI: EMBEDDING PRIVACY, FAIRNESS, AND TRANSPARENCY TO DRIVE INNOVATION AND STAKEHOLDER TRUST." Contemporary Journal of Social Science Review 1, no. 04 (2023): 1-18.

[11] iThrives Transactions on Computer Science and Engineering. “Smart Detection of Crop Pests and Diseases: Enhancing Agricultural Productivity with AI and Modern Technology”. iThrives Transactions on Computer Science and Engineering. Vol. 1. Zenodo, December 26, 2023. https://doi.org/10.5281/zenodo.17532567.

[12] S. Singh et al., "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," Journal of Ambient Intelligence and Humanized Computing, pp. 1-18, 2017.

[13] Arif, Aftab, Fadia Shah, Muhammad Ismaeel Khan, Ali Raza A. Khan, Aftab Hussain Tabasam, and Abdul Latif. 2023. “Anomaly Detection in IoHT Using Deep Learning: Enhancing Wearable Medical Device Security.” Migration Letters 20 (S12): 1992–2006.

[14] Khan, Muhammad Ismaeel, Hassan Tahir, Md Ismail Jobiullah, Ali Raza A. Khan, Sakera Begum, and Ihtasham Hafeez. "Enhancing IoT Security: A Lightweight

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

Cloning Approach for RFID/NFC Access Control Systems." Cuestiones de Fisioterapia 52, no. 2 (2023): 231-248.

[15] Jamshaid, Muhammad Mudaber, Ahmed Hassaan, Zeeshan Akbar, Muhammad Nouman Siddique, and Sikander Niaz. "IMPACT OF ARTIFICIAL INTELLIGENCE ON WORKFORCE DEVELOPMENT: ADAPTING SKILLS, TRAINING MODELS, AND EMPLOYEE WELL-BEING FOR THE FUTURE OF WORK." Spectrum of Engineering Sciences (2024).

[16] M.A. Akif, "Hybrid Machine Learning Models for Intrusion Detection in IoT," arXiv preprint arXiv:2502.12382, 2025.

[17]Tariq, Muhammad Arham, Muhammad Ismaeel Khan, Aftab Arif, Muhammad Aksam Iftikhar, and Ali Raza A. Khan. "Malware Images Visualization and Classification With Parameter Tunned Deep Learning Model." Metallurgical and Materials Engineering 31, no. 2 (2025): 68-73.https://doi.org/10.63278/1336.

[18] Zainab, Hira, Muhammad Ismaeel Khan, Aftab Arif, and Ali Raza A. Khan. "Deep Learning in Precision Nutrition: Tailoring Diet Plans Based on Genetic and Microbiome Data." Global Journal of Computer Sciences and Artificial Intelligence 1, no. 1 (2025): 31-42.

[19] Arif, Aftab, Muhammad Ismaeel Khan, and Ali Raza A. Khan. "An overview of cyber threats generated by AI." International Journal of Multidisciplinary Sciences and Arts 3, no. 4 (2024): 67-76.

[20] Khan, Muhammad Ismaeel, Aftab Arif, and Ali Raza A. Khan. "The Most Recent Advances and Uses of AI in Cybersecurity." BULLET: Jurnal Multidisiplin Ilmu 3, no. 4 (2024): 566-578.

[21] Ayub, Kahkisha, Muhammad Ahmad, Fawad Nasim, Shameen Noor, and Kinza Pervaiz. "CNN and Gaussian Pyramid-Based Approach For Enhance Multi-Focus Image Fusion." Journal of Computing & Biomedical Informatics 7, no. 02 (2024).

[22] Ahmad, Israr, Fawad Nasim, Muhammad Furqan Khawaja, Syed Asad Ali Naqvi, and Hamayun Khan. "Enhancing IoT security and services based on generative artificial intelligence techniques: a systematic analysis based on emerging threats, challenges and future directions." Spectrum of engineering sciences 3, no. 2 (2025): 1-25.

[23] N. Hamdi, "A hybrid learning technique for intrusion detection system," ScienceDirect: Journal of Information Security and Applications, 2025.

[24] K.O. Adefemi, "A Hybrid CNN-GRU Deep Learning Model for IoT Network," MDPI: Journal of Sensor and Actuator Networks, 2025.

[25] M.A. Talukder, "A hybrid machine learning model for intrusion detection in WSN and ToN-IoT," PMC: Scientific Reports, 2025.

[26] Nasim, Fawad, Sheeraz Akram, Sohail Masood, Arfan Jaffar, Muhammad Hussain Akbar, and Ch Zubair Kahloon. "Audio Source Separation: Advances and Challenges." In International Conference on Computing & Emerging Technologies, pp. 21-28. Cham: Springer Nature Switzerland, 2023.

[27] Nasim, M. F., M. Anwar, A. S. Alorfi, H. A. Ibrahim, A. Ahmed, A. Jaffar, S. Akram, A. Siddique, and H. M. Zeeshan. "Cognitively inspired sound-based automobile problem detection: A step toward explainable AI (XAI)." International Journal of Advanced and Applied Sciences 12, no. 8 (2025): 1-15.

[28] A. Kumar et al., "A Hybrid Deep Learning Framework for IoT Network Intrusion Detection System," SSRN, 2025.

[29] M. Srinivasan, "Intrusion Detection and Prevention System (IDPS) Model for IoT," IEEE Xplore, 2025.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR

[30] S.F. Misrak, "Lightweight intrusion detection system for IoT with improved hybrid deep learning," Springer: Journal of Cloud Computing, 2025.
[31] A. Qaddos, "A novel intrusion detection framework for optimizing IoT security," Nature Scientific Reports, 2024.
[32] D. Manivannan, "Recent endeavors in machine learning-powered intrusion detection," ScienceDirect: Journal of Network and Computer Applications, 2024.
nst evolving cyber threats.
[33] H. Mushtaq, A. A. Naqvi, and G. Mumtaz, "Enhancing 5G Security Preservation Through Dynamic Mixture of Experts and Transfer Learning," *Al-Aasar Journal*, vol. 2, no. 3, pp. 90-105, 2025.