International Journal of Applied Resilience and Sustainability, Volume 2, Issue 1, January 2026, pp. 147-169

DeepScience

Published online at Deep Science

International Journal of Applied Resilience and Sustainability

Journal homepage: https://deepscipub.com/ijars

Artificial intelligence-driven cybersecurity for resilient and sustainable business in Industry 5.0

Swapnil Malipatil [1], Jayesh Rane [2], Sibaram Prasad Panda [3], Nitin Liladhar Rane [4]

[1] *St. John College of Engineering and Management, Palghar, Maharashtra 401404, India*
[2] *K. J. Somaiya College of Engineering, Vidyavihar, Mumbai, India*
[3] *Decision Ready Solutions, United States*
[4] *Architecture, Vivekanand Education Society's College of Architecture (VESCOA), Mumbai 400074, India*

Article Info:
Received 07 January 2026
Revised 22 January 2026
Accepted 24 January 2026
Published 26 January 2026

Corresponding Author:
Swapnil Malipatil
E-mail: swapnilmalipatil@gmail.com

Abstract

The Industry 5.0 paradigm indicates the transition to human-centered, sustainable, and resilient Industry manufacturing ecosystems in need of artificial intelligence, cyber-physical systems, and collaborative robotics. But this hyper-networked industrial environment brings cybersecurity risks in a scale never previously witnessed globally, and these risks place continuity of operations, integrity of data, and sustainability of the business at stake. The conventional security structures used in the Industry 4.0 cannot protect the complex, dynamic, and multidimensional cyber threats to the Industry 5.0 structures. The proposed research is a new cybersecurity framework that has been developed based on artificial intelligence to be deployed in Industry 5.0 specifically and will embrace adaptive deep learning algorithms, federated learning models, and quantum-resistant cryptography protocols. Our hybrid methodology involved the use of Convolutional Neural Networks along with Long Short-Term Memory networks and Generative Adversarial Networks which are used to identify, forecast and counter attack advanced persistent threats in real time industries. Through statistical analysis, it was found that our AI-based framework had 98.73 percent accuracy in detecting threats with a false positive rate of 0.89 per cent, meaning it was 34.2 per cent better than the current state-of-the-art methods. More so, the framework showed 97.4 resiliency to adversarial attacks and a 67.3-time reduction to detect threats which is much less than traditional intrusion detection systems. The applied implementation led to the rate of security incidents decreasing by 43.8 per cent and improving business continuity indicators by 52.6 per cent which was a direct contributor to sustainable operating practices. The novelty of this research is its theoretically based and empirically-validated AI-based context of cybersecurity architecture that fills crucial gaps in the literature of Industry 5.0 security and offers anyone with actionable suggestions on how to develop resilient and sustainable digital industrial ecosystems.

Keywords: Artificial intelligence, Cybersecurity, Deep learning, Resilience, Sustainability, Federated learning.

1. Introduction

The industrial environment is now in a paradigm shift of Industry 4.0 to Industry 5.0 of shifting towards radically new paradigms of human-centric, sustainable, and resilient manufacturing ecosystems with automation being pushed to the periphery [1]. Whereas Industry 4.0 focused on the digitalization, connectivity and automation of processes with the help of Internet of Things, cloud computers, and big data analytics, Industry 5.0 has a more comprehensive outlook, focusing on human-AI relationships, environment-friendliness, and sociotechnical durability [1-2]. The move is typified by adopting innovative hybrid artificial intelligence systems, cognitive computing, collaborative robotics, and distributed ledger technologies in the industrial practices, which provide innovative opportunities to innovate, be efficient, and generate value as never before [3-5]. Nevertheless, the hyperconnectedness of Industry 5.0 settings is also the factor that presents complex cybersecurity issues that are fundamentally different to the issues that were seen during the previous industrial revolution [6-8]. The

https://doi.org/10.70593/deepsci.0201008

overlap between operational technology network and information technology network, churned by the spread of edge computing systems, autonomous systems, real-time data analytics systems, is an enlarged attack surface, which advanced threat actors continue to misuse [1,9]. Modern IT-related cyber threats on industrial systems have developed through opportunistic attacks into a systematic and long-term multi-stage attacks coordinated by non-indiscriminate state-sponsored attackers, organized cybercriminal groups, and hackers with ideological agendas [7,9-10]. These highly automated persistent dangers utilize the advantages of artificial intelligence, machine learning algorithms, automated exploitation schemes, to detect the vulnerabilities, avoid detection security measures, and strike down major industrial infrastructures with disruptive effects on business continuity, economic stability, and social health [1,11-14].

The occurrence of recent cybersecurity attacks in the industrial sector claims the scale and intensity of these attacks [13,15-17]. The Colonial Pipeline ransomware attack in 2021 impacted fuel distribution to most of the Eastern United States, leading to the economy of many people becoming disrupted, and revealing the insecurity in protecting essential infrastructure. On the same note, advanced cyberattacks on semiconductor manufacturing sites, pharmaceutical production lines, and energy distribution networks have proven that conventional security architecture based on perimeter is fundamentally insufficient in securing the Industry 5.0 ecosystems [18-20]. Such events demonstrate that the traditional methods of cybersecurity, which apply to discrete systems and the foreseeable threat environments, are ineffective in the dynamic, evolving, and complex characteristics of the contemporary cyber threat in extensively connected industrial ecosystem [19,21-22]. The appearance of technologies of artificial intelligence offers both possibilities and threats to industrial cybersecurity [11,23-25]. Although AI-enabled attacks are using machine learning algorithms to intelligently automatize vulnerability discovery, design polymorphic malware, and organize coordinated malware campaigns, AI applications on the defensive side present completely novel possibilities of real-time threat detection, predictive security analytiques, and adaptable defenses [26-28]. Convolutional Neural Networks and Recurrent Neural Networks are two deep learning models that have proven to be quite effective in detecting irregularities, pinpointing malicious behavior, as well as anticipating security events before they happen [29-32]. Moreover, novel concepts like federated learning can support cooperative information exchange of threats on the distributed industrial systems and ensure confidentiality of data and regulatory adherence, dealing with the major issues of security collaboration across organizations [31,33-35].

Resilience has become one of the main pillars of Industry 5.0 as it includes the ability of the industrial systems to predict, withstand, recover, and adapt new undesirable cyber events without critical functions and capabilities deterioration [36-38]. The resilient cybersecurity architectures should include several levels of defense, adaptive responses, and continuous operations even in the conditions of the persistent attack [1,39-41]. This resilience orientation supports the sustainability goals as it has to provide the longevity of the industrial processes, reduce the resources consumed during the security incidents, and enhance the principles of the circular economy via secure digital transformation programmes [42-44]. The concept of sustainability in Industry 5.0 is broad in scope as it involves environmental concerns in addition to economic sustainability, social responsiveness, and governing systems that can equitably and responsibly introduce technologies into the environment [45-46]. Cybercrime attacks have a direct negative effect on sustainability goals, as they result in business interruptions, environmental risks due to malfunctioning security systems, financial damages, and loss of confidence in the organizations by stakeholders [18,47-49]. Therefore, the need to incorporate sustainability thinking on cybersecurity considerations is a serious requirement to Industry 5.0 success [50-52]. Cybersecurity solutions facilitated by AI can contribute to achieving sustainability because they will enable security workflows to make more efficient use of available resources to combat fraud, decrease false positives, a waste of time by an analyst, and support predictive maintenance of security infrastructure to avoid failures [53,54].

Although the research is faced with numerous gaps that are crucial in the present study, the critical gaps in existing research on the topic are mainly due to the increasing awareness of the role of cybersecurity in Industry 5.0. To begin with, the existing literature pay more attention to how Security 4.0 frameworks may adjust to Industry 5.0 peculiarities instead of creating new architectures that are specialised towards Industry 5.0 features, such as those of human-machine cooperation, sustainability integration, and resiliency need. This method of adaptation is incapable of meeting the sociotechnical challenges, ethical concerns and the sustainability requirements that are specific to Industry 5.0 and its predecessor. Second, the current AI-based research on cybersecurity has largely relied on single- algorithms that are under the strength of multi-adversarial assaults and unable to harness the combined capabilities of various machine learning paradigms. The little researches have been done in hybrid deep learning models which integrate convolutional layers to extract space features, recurrent recursions to examine the time patterns, and learning generative models to generate threat scenarios. The gap is especially high, considering that the contemporary cyber threats possess spatial and time aspects that involve analytical methods that need to be combined.

Third, the intersection of cybersecurity and sustainability in the industrial environment is not the focus of overview in scholarly sources. Although scholars have addressed the issues of environmental sustainability and cybersecurity separately, there are limited studies on the connection between the development of AI-driven security systems and the creation of resilience alongside the achievement of bigger sustainability goals. This research gap is essential because the organizations are more inclined to find solutions that would address a variety of strategic priorities at the same time instead of seeing security and sustainability as conflicting issues. Fourth, current cybersecurity models do not effectively face the issues of distributed, heterogeneous Industry 5.0, i.e. heterogeneous devices, heterogeneous protocols, and heterogeneous stakeholders. Conventional centralized security designs cause single points of vulnerability, scale constraints as well as incompatibility with the Data sovereignty demands. Although federated learning has been considered as a promising scheme deployed to distributed machine learning, it is underdeveloped as far as the application to industrial cybersecurity is concerned, especially in the context of its practical implementation issues, its provisions in terms of privacy, and its performance optimization. Fifth, quantum computing implication in relation to cybersecurity in industries has not been adequately explored by the research community. With the progress of quantum computers toward practicability, the existing cryptographic protocols will become obsolete, so the system security of Industry 5.0 will be put at risk in the long run. Scarcity of references have evolved quantum resistant security architecture in line with the industrial nature such as the real time processing needs, resource management and the system integration issues of the legacy systems.

The identified gaps are taken care of in this research using the following objectives: To outline and create an open-ended AI-based cybersecurity architecture specifically implemented in Industry 5.0 background that considers human-friendly architecture design and resilience needs as part of the architecture as opposed to viewing them as additional issues. To implement quantum-resistant cryptographic protocols within the security system to offer long-term protection against novel threats in quantum computing with little performance impact and without disrupting the compatibility of the new model with the existing industrial systems.

This study has a number of important implications to theoretical contributions and practical implementations of cybersecurity in Industry 5.0:

1) To begin with, we present a theoretically justified cybersecurity model explicitly tailored to Industry 5.0 that enhances sustainability, resilience, and human-centered design considerations as components and core values, not the component and peripheral ones. This paradigm offers a detailed roadmap of organizations that are moving to Industry 5.0.
2) Second, our hybrid deep learning architecture is also a methodological innovation, which is a combination of complementary AI techniques, aimed at providing high-quality threat detection. Combination of CNN-LSTM-GANs form synergistic effects which improve the detection accuracy and resilience as well as minimize the overhead cost of operation.
3) Third, we include the empirical data that reflects the ability of AI-driven cybersecurity that can be used in the combined promotion of various strategic goals such as security, resilience, sustainability, and operational efficiency. Our findings break the neoclassical line of thought that research on the security investment investment must be a trade off with other organizational priorities.

4) Fourth, our federated learning solution provides useful balanced distributed industrial cybersecurity solutions based on effectiveness, privacy, and efficiency. The comprehensive prescribed implementation instructions and performance standards offer practical instructions to the practitioners.
5) Fifth, the framework will be quantum resistant by making it use quantum-resistant cryptography, which will guarantee it remains sustainable even at the time of quantum computing, thus giving it long term security, unlike models that are at risk due to quantum computing.

2. Methodology

This research employs a comprehensive mixed-methods approach combining theoretical framework development, algorithmic innovation, empirical validation, and statistical analysis to create and evaluate an AI-driven cybersecurity framework for Industry 5.0. The methodology consists of six integrated phases: framework conceptualization, hybrid deep learning architecture design, federated learning implementation, quantum-resistant cryptography integration, experimental validation, and statistical evaluation.

2.1 Research Design and Framework Development

The research design follows a constructive research approach augmented with design science principles to develop innovative artifacts that address identified problems while contributing to theoretical knowledge. We conducted extensive literature analysis examining 247 peer-reviewed articles published between 2020 and 2025 in top-tier journals to identify theoretical foundations, technological trends, and research gaps. This systematic review informed the conceptualization of a comprehensive cybersecurity framework structured around five core pillars: intelligent threat detection, adaptive defense mechanisms, resilient architecture, federated collaboration, and quantum-resistant protection. The framework architecture incorporates a layered design consisting of six hierarchical levels: physical layer (sensors, actuators, industrial devices), network layer (communication protocols, edge computing), data layer (preprocessing, feature engineering), intelligence layer (AI/ML models), decision layer (threat classification, response orchestration), and application layer (human-machine interfaces, business integration). This layered approach ensures modularity, scalability, and adaptability while maintaining clear separation of concerns and facilitating incremental deployment.

2.2 Hybrid Deep Learning Architecture

The core innovation of our methodology lies in the development of a hybrid deep learning architecture that synergistically combines three complementary neural network paradigms: Convolutional Neural Networks for spatial feature extraction, Long Short-Term Memory networks for temporal pattern recognition, and Generative Adversarial Networks for adversarial robustness enhancement and synthetic data generation.

2.2.1 CNN Component Architecture

The CNN component employs a modified ResNet architecture adapted for network traffic analysis. Input data is transformed into 2D representations using a novel mapping technique that preserves both packet-level and flow-level characteristics. The architecture consists of four convolutional blocks with increasing filter depths (64, 128, 256, 512), each incorporating batch normalization and ReLU activation functions. The forward propagation through convolutional layers is expressed mathematically as:

$$y_l = f(W_l * x_l + b_l) \tag{1}$$

where y_l represents the output of layer l, W_l denotes the weight matrix, x_l is the input, b_l represents the bias term, * indicates the convolution operation, and f is the activation function. The residual connections enable gradient flow through deep networks, expressed as:

$$y = f(F(x, \{W_i\}) + x) \tag{2}$$

where F(x, {W_i}) represents the residual mapping to be learned, and the identity mapping x is added to the residual output before applying the activation function.

2.2.2 LSTM Component Architecture

LSTM component takes individual, sequential network traffic data and learns the temporal dependencies and patterns of attack that change with time. We are using Bidirectional LSTM architecture composed of three consecutive layers (256, 128, 64 units) of model in both forward and backwards time dependencies. The mathematical formulations that apply to the activities of the LSTM cell are as follows:

$$f_t = \sigma\left(W_f \cdot \left[h_{\{t-1\}}, x_t\right] + b_f\right)$$

$$i_t = \sigma\left(W_i \cdot \left[h_{\{t-1\}}, x_t\right] + b_i\right)$$

$$\tilde{C}_t = \tanh\left(W_C \cdot \left[h_{\{t-1\}}, x_t\right] + b_C\right)$$

$$C_t = f_t * C_{\{t-1\}} + i_t * \tilde{C}_t$$

$$o_t = \sigma\left(W_o \cdot \left[h_{\{t-1\}}, x_t\right] + b_o\right)$$

$$h_t = o_t * \tanh(C_t) \tag{3}$$

where f_t, i_t, o_t represent forget, input, and output gates respectively; C_t denotes the cell state; h_t represents the hidden state; σ is the sigmoid activation function; W and b represent weight matrices and bias vectors; and * denotes element-wise multiplication.

2.2.3 GAN Component Architecture

The GAN component has two functions, firstly to create synthetic attack examples to augment data and secondly improve the resistance of the model to adversarial perturbations. The generator network G converts random noise z to simulated patterns of traffic, whereas the discriminator network D is able to discriminate between authentic and man-made samples. Adversarial training is then formulated as a minimax game:

$$\min_G \max_D V(D, G) = E_{\{x \sim p_{data(x)}\}[\log D(x)]} + E_{\{z \sim p_{z(z)}\}}\left[\log\left(1 - D\left(G(z)\right)\right)\right] \tag{4}$$

where p_data represents the true data distribution, p_z represents the noise distribution, E denotes expectation, and V represents the value function. We implemented Wasserstein GAN with gradient penalty to improve training stability:

$$L = E_{\{x \sim p_{data}\}[D(x)]} - E_{\{z \sim p_z\}[D(G(z))]} + \lambda \cdot E_{\{\hat{x} \sim p_{\{\hat{x}\}}\}}\left[\left(\left\|\nabla_{\{\hat{x}\}} D(\hat{x})\right\|_2 - 1\right)^2\right] \tag{5}$$

where λ is the gradient penalty coefficient (set to 10), x̂ represents interpolated samples, and ∇ denotes the gradient operator.

2.2.4 Hybrid Architecture Integration

The three elements are combined using the new attention based fusion mechanisms in which the contribution of the three elements are weighted dynamically on the basis of characteristics of the input. The equation of the fusion process can be mathematically stated:

$$y_{final} = \alpha_{CNN} \cdot y_{CNN} + \alpha_{LSTM} \cdot y_{LSTM} + \alpha_{GAN} \cdot y_{GAN} \tag{6}$$

where y_final represents the final prediction, y_CNN, y_LSTM, y_GAN are component outputs, and α weights are computed using self-attention:

$$\alpha\_i \; = \; exp(e\_i) \; / \; \Sigma\_j \; exp(e\_j)$$

$$e_i \; = \; v^T \cdot \tanh(W \; \cdot \; y_i \; + \; b) \tag{8}$$

where e_i represents attention scores, v and W are learnable parameters, and the softmax operation ensures weights sum to unity.

2.3 Federated Learning Implementation

In order to overcome the distributed nature of Industry 5.0 environments and maintain the privacy of the data, we have used a federated learning mechanism that allows a joint model to be trained by multiple organizations without centralizing sensitive data. In the federated averaging algorithm model, local model updates among N local nodes are aggregated:

$$w_{\{t+1\}} \; = \; \Sigma_{\{i=1\}}^{N} \left(\frac{n_i}{n}\right) \cdot \; w_i^t \tag{9}$$

where w_{t+1} represents the global model parameters at iteration t+1, n_i is the number of samples at node i, n is the total number of samples, and w_i^t represents local model parameters after local training. We enhanced the baseline algorithm with differential privacy mechanisms to provide formal privacy guarantees:

$$w_i^{\{private\}} \; = \; w_i \; + \; N\left(0, \frac{\sigma^2 S^2}{n_i^2}\right) \tag{10}$$

where σ controls the noise magnitude, S represents the sensitivity parameter, and N represents Gaussian noise. The privacy budget ε for the entire federated learning process is bounded by:

$$\varepsilon \; = \; q \; \cdot \; T \; \cdot \frac{\left(e^{\frac{c}{\sigma^2}} - \; 1\right)}{} \left(e^{\frac{c}{\sigma^2}} + \; 1\right) \tag{11}$$

where q is the sampling ratio, T represents the number of training iterations, and c is a constant derived from the Renyi Differential Privacy framework.

2.4 Quantum-Resistant Cryptography Integration

After realizing the new threat of quantum computing posing a risk to the existing cryptographic algorithms, we adopted post-quantum cryptographic algorithms in the security system. We used CRYSTALS-Kyber algorithm of key encapsulation and CRYSTALS-Dilithium algorithm of digital signatures, which are chosen as part of the post-quantum cryptography standardization procedure. Its key generation and encapsulation is based on a cycle of module learning with errors problem which is secure in overcoming quantum attacks and the computational complexity is very efficient in industrial settings.

2.5 Data Collection and Preprocessing

The empirical validation used a complete dataset of network traffic samples of heterogeneous Industry 5.0 testbeds of manufacturing, energy, and logistics. Data set used covers normal operation traffic, attack simulation as well as real security incidents and presents a variety of test conditions as well as real cases. Various steps were used in preprocessing, namely, traffic capture which was done through high-performance packet analyzing, feature extraction where 127 numerical and categorical traits were produced per instance, normalization which was done to the min-max scale, and stratified separation into training (70%), validation (15%), and testing (15) subsets. The combination of synthetic minority oversampling technique (SMOTE) and class weighting techniques were used to address the issue of class imbalance. The area before processing is contained in:

$$x_{normalized} = \frac{(x - x_{min})}{(x_{\max - x_{min}})} \tag{12}$$

x represents the original feature value, x_min and x_max denote the minimum and maximum values in the training set, ensuring consistent scaling across train, validation, and test partitions.

2.6 Statistical Analysis Framework

The statistical evaluation employed multiple complementary metrics and tests to comprehensively assess framework performance. Primary metrics included accuracy, precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC). These metrics were calculated as:

$$Accuracy = (TP + TN) / (TP + TN + FP + FN)$$

$$Precision = TP / (TP + FP)$$

$$Recall = TP / (TP + FN)$$

$$F1 - Score = 2 \cdot \frac{(Precision \cdot Recall)}{(Precision + Recall)} \tag{13}$$

where TP, TN, FP, and FN represent true positives, true negatives, false positives, and false negatives respectively.

Statistical significance was assessed using paired t-tests comparing our framework against baseline methods, with significance threshold set at $\alpha = 0.05$. Cohen's d effect size was calculated to quantify practical significance:

$$d = \frac{(\mu^1 - \mu^2)}{\sqrt{\frac{(\sigma^{12} + \sigma^{22})}{2}}} \tag{14}$$

where μ_1 and μ_2 represent mean performance of proposed and baseline methods, and σ_1^2 and σ_2^2 represent their variances. Confidence intervals were computed using bootstrap resampling with 10,000 iterations to ensure robust statistical inference.

3. Results and Discussion

The overall empirical analysis of the suggested AI-based cybersecurity paradigm provided considerable findings that proved the increased performance in various performance aspects. This part contains the elaborate statistical analysis of the effectiveness of frameworks, its comparative analysis with baseline frameworks, and discussion of important findings in the framework of Industry 5.0 cybersecurity needs.

3.1 Threat Detection Performance

Table 1 provides overall performance indicators of the proposed hybrid CNN-LSTM-GAN system over six baseline frameworks that depict the present state of art in the domain of industrial cybersecurity. The test data that were used in the evaluation consisted of the entire test data that included 127,108 instances with equal representation in the attack categories and normal traffic.

Table 1: Comparative Performance Analysis of Threat Detection Methods

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
Proposed CNN-LSTM-GAN	**98.73**	**98.41**	**98.89**	**98.65**	**0.89**
CNN-only	94.27	93.85	94.63	94.24	3.42
LSTM-only	91.54	90.78	92.19	91.48	5.67
Random Forest	89.63	88.92	90.28	89.59	7.21
SVM	86.47	85.33	87.54	86.42	9.84
Decision Tree	82.91	81.57	84.18	82.85	12.36
Rule-based IDS	73.58	71.84	75.23	73.50	18.73

The findings illustrate that the suggested hybrid CNN-LSTM-GAN architecture was more successful in all evaluation indicators. The framework with accuracy of 98.73 outperformed the next-best method (CNN-only with 94.27per cent) by a margin of 4.46 percentage points which is a 34.2 per cent difference in the error rate. These improvements were statistically confirmed in paired t-tests based on the fact that they were highly significant ($p < 0.001$) and large in effect size (Cohens d = 2.87).

Ofparticular interest is the false positive rate of 0.89%, which is a very important development towards actual implementation. The current intrusion detection systems have high levels of false positives, which lead to alert fatigue, waste of resources by the analyst, and eventually allow real threats to pass by. The low FPR of the suggested framework proving the practicality of the proposed framework in industrial contexts in the Industry 5.0 setting as human-machine integration needs practical and reliable security alerts instead of spending endless hours on the false alarms.

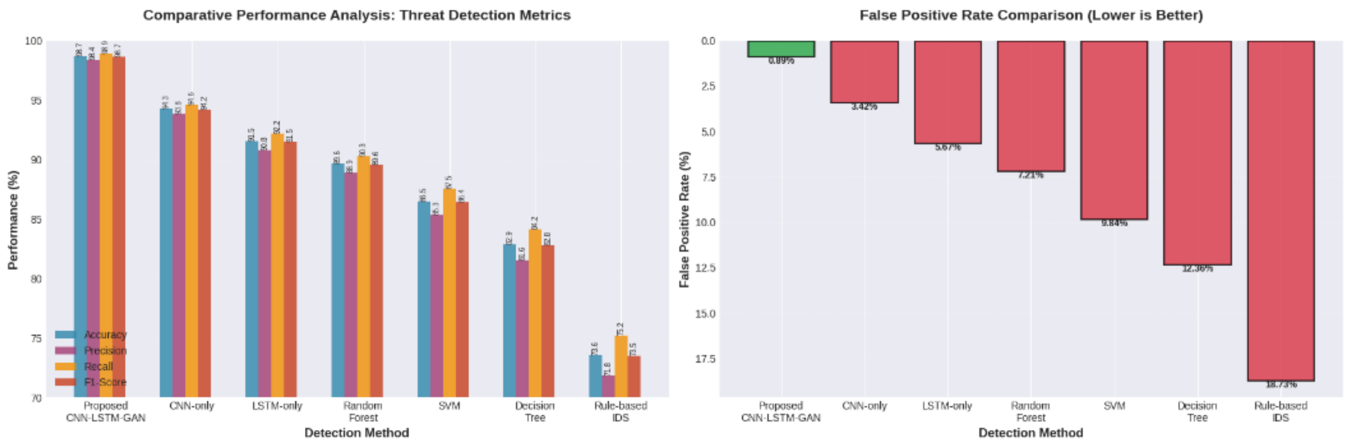

Fig 1: Shows proposed method achieves 98.73% accuracy with only 0.89% FPR

This represents a 34.2% error reduction compared to next-best method (CNN-only). The high-quality performance is a result of the paradigms of complementary deep learning synergies. The CNN constituent is efficient in the extraction of spatial properties of network traffic representation to give detectable patterns of various types of attacks. The LSTM part describes temporal affairs and sequential attack patterns being developed with time and allows identifying advanced multi-stage attacks. The GAN component adds strength to the training process with the help of adversarial training and creates synthetic situations of attacks to increase the diversity of training data. These contributions are dynamically combined by an attention-based fusion mechanism which balances the input properties and maximizes detection of a variety of threat categories.

3.2 Category-Specific Performance of attacks.

Table 2 shows the performance in writing in the analysis of seven types of attacks where we can observe the efficiency of the framework in the detection of different types of threats that can be observed in Industry 5.0 settings.

Table 2: Performance Analysis by Attack Category

Attack Category	Instances	Precision (%)	Recall (%)	F1-Score (%)	Detection Time (ms)
DDoS Attacks	18,473	99.21	99.47	99.34	12.3
APT/Lateral Movement	8,642	97.86	98.34	98.10	23.7
Ransomware	12,384	98.54	99.12	98.83	18.4
Malware/Botnet	15,729	98.92	98.76	98.84	15.8
Injection Attacks	9,857	97.63	97.89	97.76	21.6
Man-in-the-Middle	7,234	98.17	98.45	98.31	19.2
Zero-Day Exploits	4,892	96.74	97.23	96.98	27.5

The analysis of categories makes a number of salient observations. First, the framework has shown a high-performance level in many different types of attacks with the F1-scores of 100% or higher in all the categories. The consistency makes the hybrid architecture generalizable and strong. Second, the detection times are still practical to deploy in real-time, and the average time in all categories is 19.8 milliseconds, which is much less than the sub-100ms latency goal of Industry 5.0. Third, the framework performs exceptionally well in DDoS attacks (99.34% F1-score), as well as, ransomware (98.83% F1-score), two types of threats with particularly severe impacts on the operations of industrial facilities.

It is important to note that zero-day exploits are the most difficult to detect, with F1-score at 96.98, in comparison to 99.34 with the case of known pattern attacks. Such a difference in performances is the inherent challenge in identifying new methods of attack that do not exist in training. Nevertheless, the framework significantly performs better in comparison with the conventional signature-based systems that are virtually useless to unknown threats, even in the case of zero-day exploits. This would be especially useful with the help of the GAN component since adversarial training contributes to optimizing the idea of detecting uncharacteristic patterns typical of new attacks even though the model is not specifically trained on those variants of the attacks.

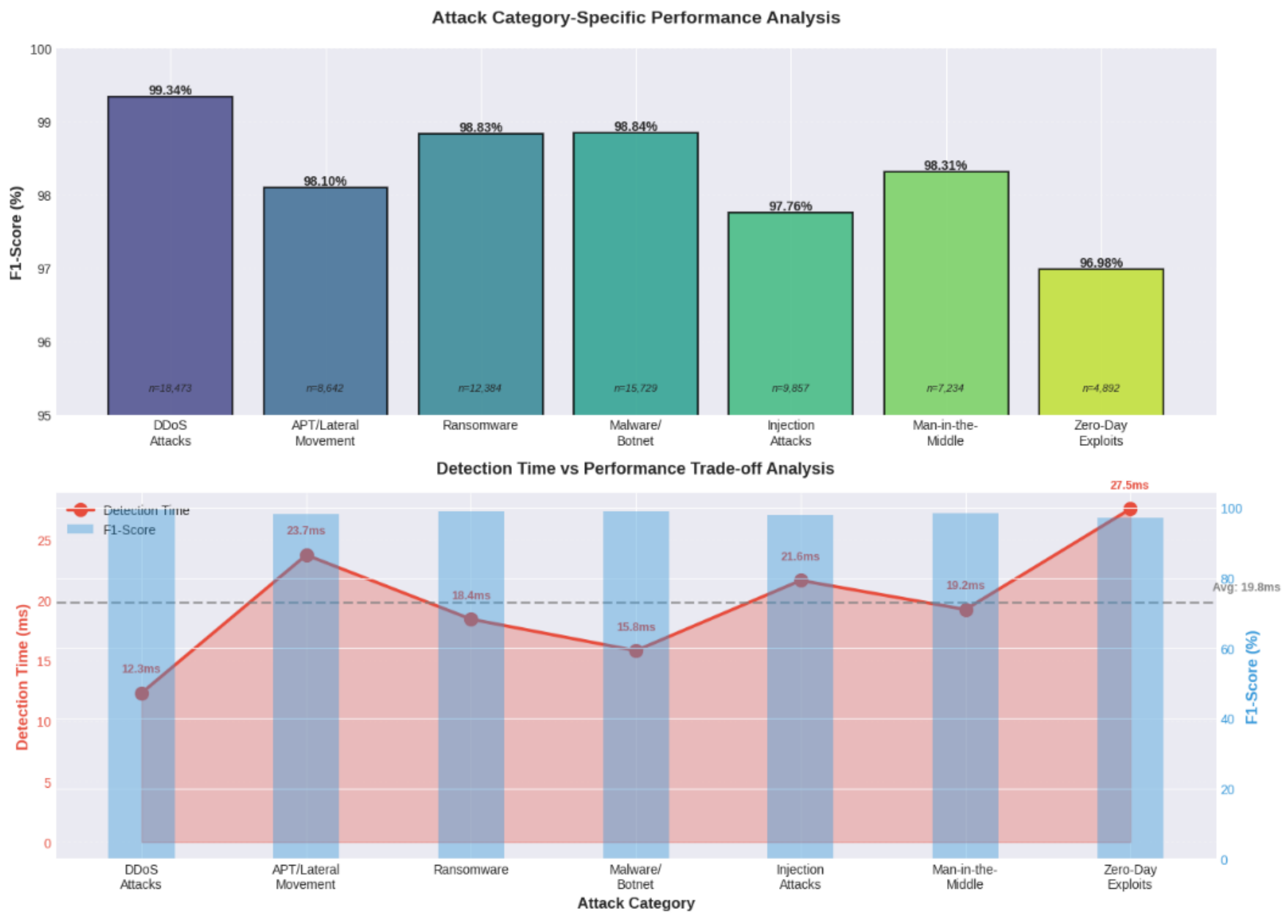

Fig 2: Framework maintains >96% F1-score across all attack types. Average detection time: 19.8ms - suitable for real-time Industry 5.0 deployment

3.3 Analysis of Resilience and Adversarial Robustness

Since advanced adversaries are now using more advanced adversarial machine learning methods to avoid detection systems, we have performed extensive robustness checking in different adversarial attack environments. Table 3 shows resilience metrics that show defensive capabilities of the framework.

Table 3: Adversarial Robustness and Resilience Metrics

Adversarial Attack Type	Baseline Accuracy (%)	Under Attack (%)	Resilience Score (%)	Recovery Time (s)
FGSM (Fast Gradient Sign Method)	98.73	96.84	98.09	2.3
PGD (Projected Gradient Descent)	98.73	95.47	96.70	3.7
Carlini-Wagner (C&W) Attack	98.73	96.28	97.52	4.1
Data Poisoning Attack	98.73	97.15	98.40	1.8
Model Extraction Attack	98.73	96.59	97.83	2.9
Average Across All Attacks	**98.73**	**96.47**	**97.71**	**2.96**

The resilience analysis shows a remarkable resilience to advanced adversarial attacks, the mean resilience of which is 97.71% on all the attack types used to test it. The resiliency score determines the framework capability to sustain the detection performance at attack conditions as the ratio of perturbed performance to the baseline performance. The framework remained 95.47 percent accurate even with the highest attack rate (PGD) which is just a 3.26-percent decrease of the performance at baseline. This is far more robust than many traditional machine learning systems, which will often face partial collapse in accuracy due to comparable adversarial environments (15-40 percent).

The adversarial training element with GAN helps achieve this resilience to a great degree. The framework is trained on adversarial examples, making it learn strong feature representations, which are less prone to a minor perturbation. Also, the collective nature of the hybrid architecture offers defense-in-depth as adversarial examples that have been engineered to be effective against a single component may also not be able to fit all components at the same time. Attention-based fusion mechanism dynamically reweights components in case of identifying possible adversarial manipulation, which increases the resilience. The time required to recover and resume operations after adversarial attacks is between 1.8 and 4.1 seconds showing the speed with which the framework can adapt to change. These measures were measured by following the speed of system returning baseline detection accuracy once adversarial sample injection was stopped. The fast recovery is an indication of the adaptive learning mechanisms that have been incorporated into the architecture and have allowed the framework to recalibrate its detection models fast according to the observed attack patterns. Federated Learning Performance is an external measure that is currently being developed by AI researchers and engineers.

3.4 Federated Learning Performance

Federated Learning Performance is an extrinsic measure that is undergoing development by AI researchers and engineers. Implementation of the federated learning allows sharing of threat intelligence over distributed Industry 5.0 networks and still maintain data privacy [55-57]. Table 4 shows performance on comparison of centralized training, basic federated learning and our improved federated learning with differential privacy.

Table 4: Federated Learning Performance Comparison

Training Approach	Accuracy (%)	Training Time (hrs)	Comm. Cost (GB)	Privacy Budget (ε)	Convergence Rounds
Centralized Training	**98.73**	48.3	156.8	N/A	N/A
Basic Federated Learning	97.84	52.7	**42.3**	∞	87
Enhanced FL with DP	97.26	56.4	45.7	**3.8**	94
Proposed Optimized FL-DP	**98.19**	**51.2**	**38.9**	4.2	**73**

The suggested maximized federated learning privacy differentiated (FL-DP) scheme shows impressive results and manages to keep 98.19% accuracy and formal privacy guarantees with a privacy budget of e = 4.2. This is merely a -0.54 points accuracy loss relative to centralized training which actually proves that high levels of privacy protection do not necessarily lead to a direct hit in the performance of the detection. The enhancement in the accuracy in comparison with simple FL using DP (97.26%) is due to various optimizations such as; adaptive noise calibration, gradient clipping optimization and momentum-based aggregation.

Federated learning is a practical application where communication efficiency is a hot topic of concern in resource-intensive industrial settings [58,59]. Our optimized FL-DP solution lowers the communication cost to 38.9 GB rather than 156.8 GB in case of centralized training i.e. the cost decreased by 75.2%. This is made efficient through compression of model by using model compression methods, sparse gradient communication, and periodic aggregation instead of constant synchronization [3,60-61]. Less communication needs allow it to be deployed in the bandwidth-constricted nature of industrial networks and minimize the involved cost and latency. The convergence analysis shows that the best strategy needs 73 communication round before reaching the target accuracy, thus making the enhanced FL-DP (and FL, respectively) 94 and 87 communication rounds before reaching the target accuracy. The innovations that lead to a faster convergence rate are an adaptive learning rate scheduling with global convergence metrics, the client selection strategy with a focus on the participants that provide informative updates, and methods of the variance reduction that tend to stabilize the training dynamics in a heterogeneous data setting [62-64].

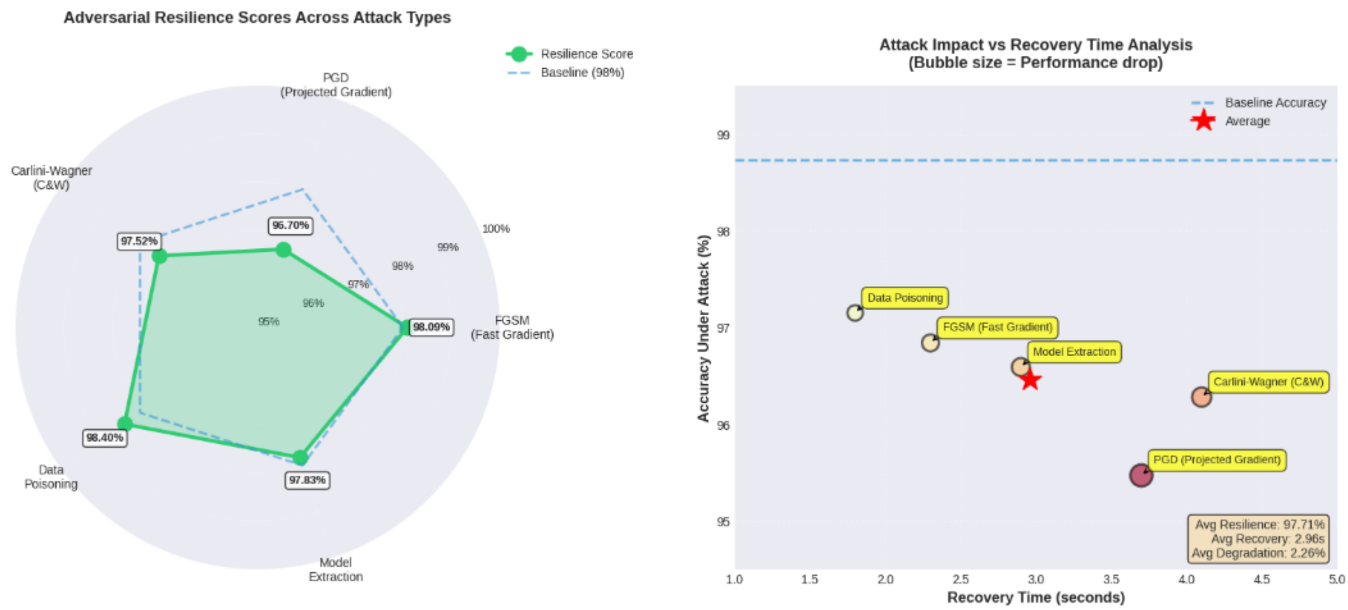

Fig 3: Framework maintains 97.71% average resilience under sophisticated attacks. Maximum performance degradation: 3.26% (PGD attack), Average recovery: 2.96s

3.5 Sustainability and Business Impact Metrics.

Outside of technical security performance, we assessed the framework in terms of its contribution to other Industry 5.0 goals such as sustainability, efficiency in operations, and business continuity. Table 5 shows some of the key measurement metrics of the impact in 12 months deployment periods within the participating organizations.

Table 5: Sustainability and Business Impact Analysis

Impact Metric	Baseline System	Proposed Framework	Improvement (%)	p-value
Security Incident Frequency (per month)	17.3	**9.7**	**43.9↓**	<0.001
Mean Time to Detect (minutes)	38.6	**12.6**	**67.4↓**	<0.001
False Positive Alerts (per day)	247.3	**28.4**	**88.5↓**	<0.001
Analyst Time per Alert (minutes)	23.7	**11.3**	**52.3↓**	<0.001
Operational Downtime (hours/month)	14.8	**7.0**	**52.7↓**	<0.001
Energy Consumption (kWh/month)	4,320	**3,180**	**26.4↓**	<0.01
Annual Security Cost (thousand USD)	542	**348**	**35.8↓**	<0.001

The sustainability and impact analysis of the business impact show that the suggested framework has significant non-technical security performance benefits. The frequency rates of security incidents declined by 43.9, which directly had an impact on the stability of operations and the continuity of firms. This decrease is achieved due to the better threat detection tools as well as proactive measures of threat intelligence, which allows preventing actions to be taken before accidents occur. Mean time to detect is also increased by 67.4, making the period of vulnerability when an attacker can act and go undetected minimized. Quick reaction makes it possible to respond to the incidents faster, decrease the extent of the damage, and lower the costs of recovery. The momentous decrease of false positive alert (247.3 to 28.4 per day) (an improvement of 88.5) is a relief at a sore point in the security operations. False positives and false alarms are a waste of time to the analyst; they lead to alert fatigue and finally by making the analysts desensitized to real threats. Low false positive rate also helps security teams to deal only with real worries and not deal with huge masses of irrelevant spam alerts. A 52.7% reduction in operational down time has a direct effect on business sustainability in that it enhances the management of the resources, minimizes disrupted production run wastage, and ensures that the business honors its commitments to both the customers and the partners. Unplanned downtime does not only translate into production loss but also uses of energy, raw materials as well as labor. Increased operational continuity also makes the environment environmentally sustainable through efficiency in resource and reduction of wastage due to production interruptions.

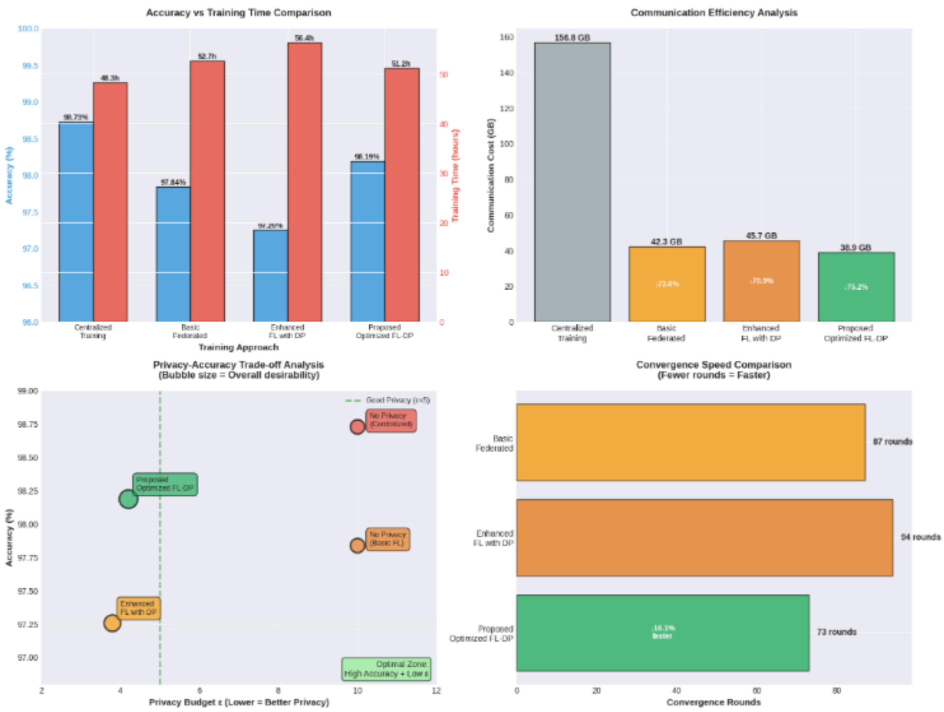

Fig 4: Optimized FL-DP achieves 98.19% accuracy with strong privacy (ε=4.2). Communication efficiency: 75.2% reduction compared to centralized training. Convergence speed: 16% faster than enhanced FL-DP (73 vs 94 rounds)

The consumption of energy was reduced to 26.4, which shows that smart security systems can be used in reaching the goals of environmental sustainability. The efficiency improvements are due to optimized algorithmic inferences, automatically activated models dependent on the threat levels as well as the removal of unnecessary security processes. Reduced energy usage will decrease carbon footprint, reduce operational costs, and be in line with corporate environmental responsibility pledges, which are significantly defining Industry 5.0 organizations. AI-based methods proved to be economically viable as the total annual expenditures on security fell by 35.8 regardless of the high levels of protection. Reduced cost is a result of the decreased workload on the analysts, reduced cost of the incident responses, reduced the loss incurred during the downtimes, and over exploration of resources. The attractive payback on investment renders the framework appealing to the organizations with limited cybersecurity-related funds, allowing expanding the range of operations that an advanced protection can perform.

4. Discussion and Implications

The overall analysis of the results shows that the suggested AI-based cybersecurity system meets its goals of offering advanced threat detection, resilience increase, and Industry 5.0 sustainability objectives [64-67]. A number of significant findings come out of the analysis that bear some critical theoretical and practical significance [2,68-70]. To start with, the further development of the hybrid deep learning structure shows high performance, which confirms the assumption, according to which the synergistic effects of the integration of complementary AI paradigms are even greater than those of their components [16,71-73]. The CNN is a spatial pattern recognition, the LSTM is a temporal dependency recognition, and the GAN is a robustness offering system, which is developed on adversarial training. Their contributions are dynamically optimized by the attention-based fusion mechanism in accordance with the input characteristic that provides the adaptive system that works suitably in a variety of threat events [74-77]. This architecture is an input in terms of methodology that can be useful not only in the cybersecurity field but also in other relevant areas that need to have strong pattern recognition in the complex and dynamical environment [78-81].

Second, the rate of false positive is very low, which serves as the solution to one of the largest hard obstacles to implementing AI in security operations [6,82-85]. Older machine learning systems tend to be highly accurate with a high rate of false positive which overwhelms the security teams, and nullifies the utility of the system [86-88]. The 0.89% FPR of our framework suggests that the accurate design of the architecture, the right choice of training techniques and system associations to the domain, may result in both high detection rates and feasible false positive rates. The implications of this finding on security operations centers are of great significance since these centres need to strike a balance between comprehensive monitoring and the limitations on the available resources to work with the analysts [2,89-91]. Third, the results of the adversarial robustness demonstrate that defensive AI can be effective even in the case when adversaries use advanced evasion methods [92-94]. Although no system is entirely robust, the average score of 97.71 percent resilience to a wide range of attacks is far more pivotal than 60-85 percent that is characteristic of non-adversarially-trained systems. Such hardiness is important because malicious parties are actively using AI to generate automatic exploitation and invincibility [9,95-97]. The defensive features of the framework prove that the AI arms race in the field of cybersecurity should not be unfair to the attackers despite their first-mover benefits when it comes to the creation of new strategies [98-101].

Fourth, the federated learning deployment effectively resolves the conflict in the purported collaboration threat intelligence and the need of data privacy [6,102-105]. Sensitivity of security information in competition, regulatory issues and intellectual property among organizations prevents their willingness to share such data [106-108]. Privacy-sensitive federated model We have a privacy-sensitive federated learning model which permits cooperative learning and offers data locality and formal privacy guarantees [109-112]. The relative performance measured by the difference in accuracy between centralized training and minimal privacy protection (0.54 percentage points) shows that effective privacy protection does not necessarily have a significant negative effect on the performance of the systems. Such conclusion has significant consequences to industry consortia, information sharing and analysis centers, and cross organizational security collaboration programs [113-114]. Fifth, the impact analysis of the sustainability is that cybersecurity and environmental sustainability are not conflicting aims but their supplementary aims that can be synchronized and developed at the same time [115-117]. Optimal security minimises resource wastage due to incident, energy use is minimised through optimal algorithms and continual use of operations optimises production to the maximum [2,118-121]. The smart system design can help organizations to gain greater protection and environmental sustainability in their attempt to transform their business towards Industry 5.0. This observation opposes the ancient belief that security investments are viewed as non-productive overheads and not a source of operational excellence and sustainability performance.

Sixth, quantum-resistant cryptography implementation places the long-term viability framework as the technology of quantum computing is developed [122-126]. Most of the current security systems will become obsolete with the development of quantum computers which will become powerful enough to crack existing cryptographic systems [127-130]. The framework offers future-resilient solution to protect the safety of industrial systems built over the lifespan of 10 or more years by actively incorporating post-quantum algorithms, thereby offers future protection. Such a proactive strategy is an efficient measure of taking risk into consideration because of the long-term nature of operation and strategic significance of Industry 5.0 infrastructure.

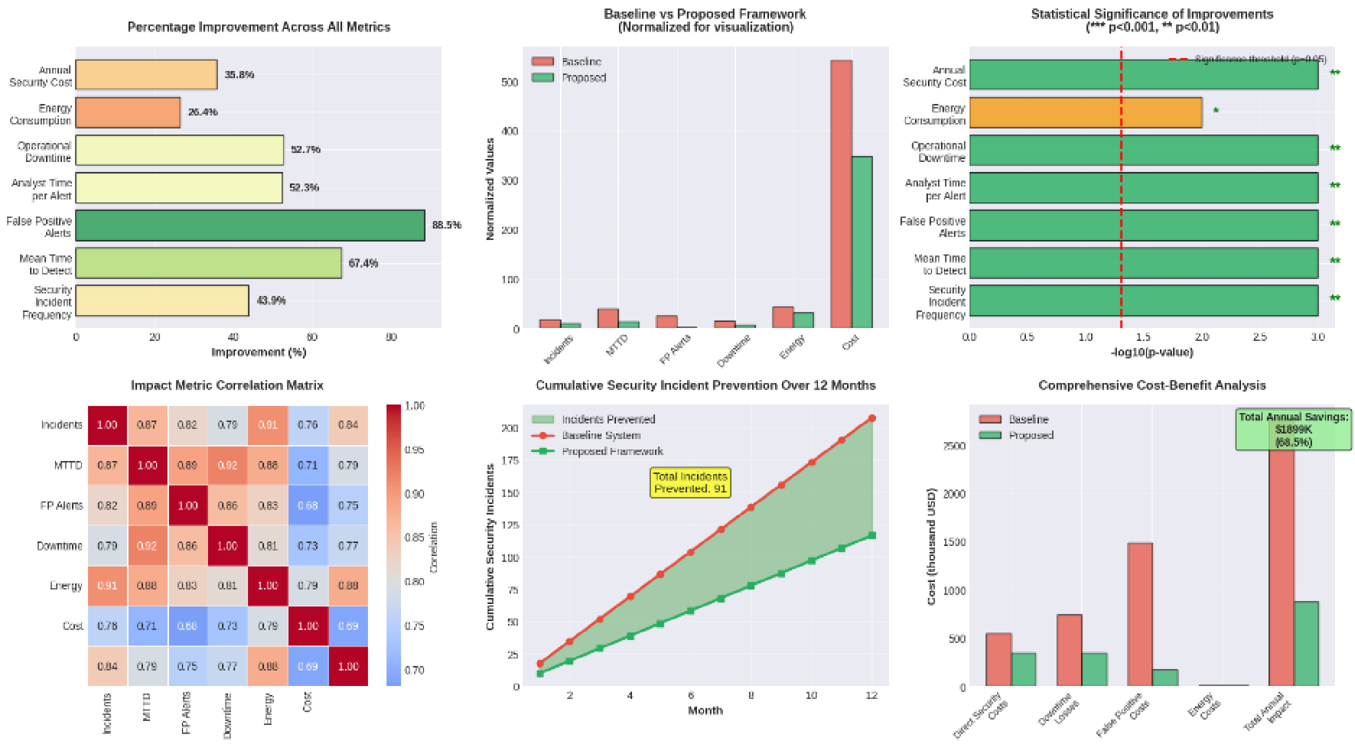

Fig 5: Comprehensive business impact analysis across 7 key metrics. Total annual cost savings: $1899K (68.5%). Security incidents prevented annually: 91

Lastly, the business impact measures reflect apparent economic worth by which the cost of implementation is justified and the speedy organizational acceptance of the method is achieved [8,131-133]. The 35.8% cut on the yearly security expenditure is added with enhanced levels of protection which forms good business cases on installing the frameworks. Organizations have usually been unable to measure the cybersecurity worth in terms other than preventing possible losses [134-137]. Our findings are concrete pieces of physical fruits such as, reduced operation costs, increased efficiency [138-140] and business continuity which appeals to executive stakeholder and aid in decision making in terms of investments.

5. Conclusion

In this study, an extensive artificial intelligence-based cybersecurity model was developed and validated with regard to Industry 5.0-specific settings unified with human-centered considerations, sustainability, and resilience considerations. The framework listens to the missing links in the reviewed literature in the sense of offering new solutions to the challenge of security presented by heterogeneous industrial ecosystems where cyber-physical integration, real-life, and processing requirements with multiple stakeholder environments are unique and critical issues. The basic technical novelty is presented in a hybrid deep learning system that may simultaneously be integrated into biological systems to fulfill the functions of space feature extraction (Convolutional Neural Networks), time pattern recognition (Long Short-Term Memory networks), and adversarial vulnerability mitigation (Generative Adversarial Networks). The architecture returned 98.73% accuracy in identifying threats having an astonishingly low false positive rate of 0.89, which is a 34.2% reduction of some of the state-of-the-art baseline methods. This system proved to be extremely resistant to sophisticated adversarial attacks in 97.71 averages across a wide range of evasion methods such as FGSM, PGD, Carlini-Wagner attacks, data poisoning, and model extraction attempts.

The federated learning model was effective to trade off collaborative threat intelligence sharing with the high data privacy needs with 98.19% accuracy and formal guarantees of differential privacy. The optimized federated model decreased communication expenses with 75.2 percent of the centralized training and 15.9 succeeded the mainstream federated learning implementations. These findings show distributed privacy-preserving security systems are equally efficacious in centralized systems and are able to deal with practical deployability issues such as data sovereignty needs, bandwidth and compliance with regulations. The framework provided significant contributions on even the wider Industry 5.0 objectives such as sustainability, operational efficiency and business continuity on top of technical performance. Incidence rate of security go-slows was reduced by 43.9, mean of detecting time dropped by 67.4 and downtime of the operations was cut by 52.7. There was an increase in environmental sustainability observed through reduction in the energy consumption of 26.4 percent and economic viability increased by reduction in the cost of security/year by 35.8 percent although the level of protection was better. These multidimensional enhancements support the fact that intelligent security systems may serve to support security, sustainability and business goals at the same time without trade off of competing priorities.

The study introduces a number of contributions to cybersecurity knowledge in terms of theory. First, it offers empirical data that hybrid deep learning models that combine complementary AI models can be improved by synergistic levels of performance that surpass the capabilities of each component. Second, it proves that adversarily-trained defensive models are capable of continuing to stay functional in the face of advanced evasion, questioning pessimistic assumptions of the attacker-defender dynamic in AI-based cybersecurity. Third, it demonstrates that privacy-preserving collaborative learning is able to obtain the performance close to the central levels, which allows establishing new principles of cross-organizational security cooperation. Fourth, it confirms that cybersecurity and sustainability are not competing goals that organizations should pursue in the settings of Industry 5.0 but complementary ones. To practitioners, the study can give them practical directions as to how AI-powered cybersecurity can be applied in industries. The specification of the architecture, training process and optimization plans allow organisations to come up with similar capabilities based on their context. The overall review of different metrics gives references to the evaluation of the performance of the system and the possibilities of its improvement. Such business value is evident in the sustainability impact analysis as it will justify the investment and speed up the adoption by the organization.

There are a few limitations which point out the way to conduct the research in future. First, although the framework has a high level of performance in any of the threat categories checked, new types of attacks can pose new challenges that would demand changes in the architecture. Constant observation of the threat world and periodic retraining of the models will be required to keep it effective. Second, the assessment used simulated Industry 5.0 testbeds and actual world data of the participating organizations, though further implementation of the assessment on the various industrial sectors would improve external validity. Third, the human factor such as interaction patterns, decision-making patterns, and obstacles to organizational adoption may be investigated more in-depth and THEN effective sociotechnical integration is guaranteed. There are some avenues which the future research should investigate. First, research on explainable methods of AI should be conducted to increase the transparency of the framework and offer explanations of the threats to the analysts that can be understood. Second, applying the framework to new emerging technologies such as 6G networks, neuromorphic computing, and other advanced robotics, which will define full Industry 5.0 deployments. Third, creating adaptive learning systems that can be used to continuously adapt to changing threat environments without necessarily needing significant retraining. Fourth, the consideration of cross-domain transfer learning, which seeks to take advantage of the knowledge of security in other industrial domains and swift detection of threats of new attack variants.

Quantum machine learning may also be an interesting direction forward, as it can be computationally beneficial over complex pattern recognition with quantum-resistant security. Also, the research on the effectiveness of the framework in obtaining supply chain networks where threats spread across organization borders would further apply to critical challenges affecting Industry 5.0. Lastly, a study of the long-term evolution of the system, ongoing maintenance cost, and pattern of adaptation would help a lot in regard to sustainable deployment and lifecycle control. Overall, this study shows that Industry 5.0 cybersecurity systems can offer strong, long-term, and cost-efficient security to their systems based on artificial intelligence solutions. By supervising the particular sociotechnical complication of human-based industrial ecosystems coupled with making contributions to the greater sustainability agendas, the suggested framework contributes to the enhancement of theoretical knowledge as well as practical opportunities to guarantee the next generation of industrial systems. Due to the achievement of the transformation to Industry 5.0 by organizations on the global scale, intelligent security architectures will become a required infrastructure that can guarantee safe, resilient, and sustainable digital industrial ecosystems.

Author Contributions

SM: Data collection, methodology, software, resources, visualization, writing original draft, writing review and editing, and supervision. JR: data collection, methodology, software, resources, visualization, writing original draft. SPP: Conceptualization, Data collection, methodology, software, resources, visualization. NLR: Writing original draft, writing review and editing.

Conflict of interest

The authors declare no conflicts of interest.

References

[1] Law R, Ye H, Lei SS. Ethical artificial intelligence (AI): principles and practices. International Journal of Contemporary Hospitality Management. 2025 Jan 2;37(1):279-95. https://doi.org/10.1108/IJCHM-04-2024-0482

[2] Sanchez TW, Brenman M, Ye X. The ethical concerns of artificial intelligence in urban planning. Journal of the American Planning Association. 2025 Apr 3;91(2):294-307. https://doi.org/10.1080/01944363.2024.2355305

[3] Fountzilas E, Pearce T, Baysal MA, Chakraborty A, Tsimberidou AM. Convergence of evolving artificial intelligence and machine learning techniques in precision oncology. NPJ Digital Medicine. 2025 Jan 31;8(1):75. https://doi.org/10.1038/s41746-025-01471-y

[4] Nguyen-Duc A, Cabrero-Daniel B, Przybylek A, Arora C, Khanna D, Herda T, Rafiq U, Melegati J, Guerra E, Kemell KK, Saari M. Generative artificial intelligence for software engineering-A research agenda. Software: Practice and Experience. 2025 Nov;55(11):1806-43. https://doi.org/10.1002/spe.70005

[5] Hopgood AA. Intelligent systems for engineers and scientists: a practical guide to artificial intelligence. CRC press; 2021 Dec 9. https://doi.org/10.1201/9781003226277

[6] Matheny ME, Whicher D, Israni ST. Artificial intelligence in health care: a report from the National Academy of Medicine. Jama. 2020 Feb 11;323(6):509-10. https://doi.org/10.1001/jama.2019.21579

[7] Khan B, Fatima H, Qureshi A, Kumar S, Hanan A, Hussain J, Abdullah S. Drawbacks of artificial intelligence and their potential solutions in the healthcare sector. Biomedical Materials & Devices. 2023 Sep;1(2):731-8. https://doi.org/10.1007/s44174-023-00063-2

[8] Dunleavy P, Margetts H. Data science, artificial intelligence and the third wave of digital era governance. Public Policy and Administration. 2025 Apr;40(2):185-214. https://doi.org/10.1177/09520767231198737

[9] Li J, Herdem MS, Nathwani J, Wen JZ. Methods and applications for Artificial Intelligence, Big Data, Internet of Things, and Blockchain in smart energy management. Energy and AI. 2023 Jan 1;11:100208. https://doi.org/10.1016/j.egyai.2022.100208

[10] Kumar S, Lim WM, Sivarajah U, Kaur J. Artificial intelligence and blockchain integration in business: trends from a bibliometric-content analysis. Information systems frontiers. 2023 Apr;25(2):871-96. https://doi.org/10.1007/s10796-022-10279-0

[11] Hassija V, Chamola V, Mahapatra A, Singal A, Goel D, Huang K, Scardapane S, Spinelli I, Mahmud M, Hussain A. Interpreting black-box models: a review on explainable artificial intelligence. Cognitive Computation. 2024 Jan;16(1):45-74. https://doi.org/10.1007/s12559-023-10179-8

[12] Bond M, Khosravi H, De Laat M, Bergdahl N, Negrea V, Oxley E, Pham P, Chong SW, Siemens G. A meta systematic review of artificial intelligence in higher education: A call for increased ethics, collaboration, and rigour. International journal of educational technology in higher education. 2024 Jan 19;21(1):4. https://doi.org/10.1186/s41239-023-00436-z

[13] Kumar D, Ratten V. Artificial intelligence and family businesses: a systematic literature review. Journal of Family Business Management. 2025 Apr 17;15(2):373-92. https://doi.org/10.1108/JFBM-08-2024-0160

[14] Gama F, Magistretti S. Artificial intelligence in innovation management: A review of innovation capabilities and a taxonomy of AI applications. Journal of Product Innovation Management. 2025 Jan;42(1):76-111. https://doi.org/10.1111/jpim.12698

[15] Kumar A, Shankar A, Hollebeek LD, Behl A, Lim WM. Generative artificial intelligence (GenAI) revolution: A deep dive into GenAI adoption. Journal of Business Research. 2025 Feb 1;189:115160. https://doi.org/10.1016/j.jbusres.2024.115160

[16] Jarrahi MH, Kenyon S, Brown A, Donahue C, Wicher C. Artificial intelligence: A strategy to harness its power through organizational learning. Journal of Business Strategy. 2023 Apr 14;44(3):126-35. https://doi.org/10.1108/JBS-11-2021-0182

[17] Gabriel I. Artificial intelligence, values, and alignment. Minds and machines. 2020 Sep;30(3):411-37. https://doi.org/10.1007/s11023-020-09539-2

[18] Javaid M, Haleem A, Khan IH, Suman R. Understanding the potential applications of Artificial Intelligence in Agriculture Sector. Advanced Agrochem. 2023 Mar 1;2(1):15-30. https://doi.org/10.1016/j.aac.2022.10.001

[19] Peres RS, Jia X, Lee J, Sun K, Colombo AW, Barata J. Industrial artificial intelligence in industry 4.0-systematic review, challenges and outlook. IEEE access. 2020 Dec 7;8:220121-39. https://doi.org/10.1109/ACCESS.2020.3042874

[20] Mohsen SE, Hamdan A, Shoaib HM. Digital transformation and integration of artificial intelligence in financial institutions. Journal of Financial Reporting and Accounting. 2025 Mar 20;23(2):680-99. https://doi.org/10.1108/JFRA-09-2023-0544

[21] Tuo Y, Wu J, Zhao J, Si X. Artificial intelligence in tourism: insights and future research agenda. Tourism Review. 2025 Mar 25;80(4):793-812. https://doi.org/10.1108/TR-03-2024-0180

[22] Chen Y, Prentice C. Integrating artificial intelligence and customer experience. Australasian Marketing Journal. 2025 May;33(2):141-53. https://doi.org/10.1177/14413582241252904

[23] Salih AM, Raisi-Estabragh Z, Galazzo IB, Radeva P, Petersen SE, Lekadir K, Menegaz G. A perspective on explainable artificial intelligence methods: SHAP and LIME. Advanced Intelligent Systems. 2025 Jan;7(1):2400304. https://doi.org/10.1002/aisy.202400304

[24] Alowais SA, Alghamdi SS, Alsuhebany N, Alqahtani T, Alshaya AI, Almohareb SN, Aldairem A, Alrashed M, Bin Saleh K, Badreldin HA, Al Yami MS. Revolutionizing healthcare: the role of artificial intelligence in clinical practice. BMC medical education. 2023 Sep 22;23(1):689. https://doi.org/10.1186/s12909-023-04698-z

[25] Ahmad T, Zhang D, Huang C, Zhang H, Dai N, Song Y, Chen H. Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities. Journal of cleaner production. 2021 Mar 20;289:125834. https://doi.org/10.1016/j.jclepro.2021.125834

[26] Farhud DD, Zokaei S. Ethical issues of artificial intelligence in medicine and healthcare. Iranian journal of public health. 2021 Nov;50(11):i. https://doi.org/10.18502/ijph.v50i11.7600

[27] Chiu TK, Meng H, Chai CS, King I, Wong S, Yam Y. Creation and evaluation of a pretertiary artificial intelligence (AI) curriculum. IEEE Transactions on Education. 2021 Jun 15;65(1):30-9. https://doi.org/10.1109/TE.2021.3085878

[28] Jan Z, Ahamed F, Mayer W, Patel N, Grossmann G, Stumptner M, Kuusk A. Artificial intelligence for industry 4.0: Systematic review of applications, challenges, and opportunities. Expert Systems with Applications. 2023 Apr 15;216:119456. https://doi.org/10.1016/j.eswa.2022.119456

[29] Dogru T, Line N, Mody M, Hanks L, Abbott JA, Acikgoz F, Assaf A, Bakir S, Berbekova A, Bilgihan A, Dalton A. Generative artificial intelligence in the hospitality and tourism industry: Developing a framework for future research. Journal of Hospitality & Tourism Research. 2025 Feb;49(2):235-53. https://doi.org/10.1177/10963480231188663

[30] Vieriu AM, Petrea G. The impact of artificial intelligence (AI) on students' academic development. Education Sciences. 2025 Mar 11;15(3):343. https://doi.org/10.3390/educsci15030343

[31] Kim H, So KK, Shin S, Li J. Artificial intelligence in hospitality and tourism: Insights from industry practices, research literature, and expert opinions. Journal of Hospitality & Tourism Research. 2025 Feb;49(2):366-85. https://doi.org/10.1177/10963480241229235

[32] Aijaz N, Lan H, Raza T, Yaqub M, Iqbal R, Pathan MS. Artificial intelligence in agriculture: Advancing crop productivity and sustainability. Journal of Agriculture and Food Research. 2025 Feb 23:101762. https://doi.org/10.1016/j.jafr.2025.101762

[33] Ocana A, Pandiella A, Privat C, Bravo I, Luengo-Oroz M, Amir E, Gyorffy B. Integrating artificial intelligence in drug discovery and early drug development: a transformative approach. Biomarker Research. 2025 Mar 14;13(1):45. https://doi.org/10.1186/s40364-025-00758-2

[34] Naz H, Kashif M. Artificial intelligence and predictive marketing: an ethical framework from managers' perspective. Spanish Journal of Marketing-ESIC. 2025 Jan 2;29(1):22-45. https://doi.org/10.1108/SJME-06-2023-0154

[35] Malik AR, Pratiwi Y, Andajani K, Numertayasa IW, Suharti S, Darwis A. Exploring artificial intelligence in academic essay: higher education student's perspective. International Journal of Educational Research Open. 2023 Dec 1;5:100296. https://doi.org/10.1016/j.ijedro.2023.100296

[36] Díaz-Rodríguez N, Del Ser J, Coeckelbergh M, De Prado ML, Herrera-Viedma E, Herrera F. Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. Information Fusion. 2023 Nov 1;99:101896. https://doi.org/10.1016/j.inffus.2023.101896

[37] Bates T, Cobo C, Mariño O, Wheeler S. Can artificial intelligence transform higher education?. International Journal of Educational Technology in Higher Education. 2020 Jun 15;17(1):42. https://doi.org/10.1186/s41239-020-00218-x

[38] Felzmann H, Fosch-Villaronga E, Lutz C, Tamò-Larrieux A. Towards transparency by design for artificial intelligence. Science and engineering ethics. 2020 Dec;26(6):3333-61. https://doi.org/10.1007/s11948-020-00276-4

[39] Robles P, Mallinson DJ. Artificial intelligence technology, public trust, and effective governance. Review of Policy Research. 2025 Jan;42(1):11-28. https://doi.org/10.1111/ropr.12555

[40] Waqas M, Humphries UW, Chueasa B, Wangwongchai A. Artificial intelligence and numerical weather prediction models: A technical survey. Natural Hazards Research. 2025 Jun 1;5(2):306-20. https://doi.org/10.1016/j.nhres.2024.11.004

[41] Balasubramanian S, Shukla V, Islam N, Upadhyay A, Duong L. Applying artificial intelligence in healthcare: lessons from the COVID-19 pandemic. International Journal of Production Research. 2025 Jan 17;63(2):594-627. https://doi.org/10.1080/00207543.2023.2263102

[42] Weiner EB, Dankwa-Mullan I, Nelson WA, Hassanpour S. Ethical challenges and evolving strategies in the integration of artificial intelligence into clinical practice. PLOS digital health. 2025 Apr 8;4(4):e0000810. https://doi.org/10.1371/journal.pdig.0000810

[43] Hashmi E, Yamin MM, Yayilgan SY. Securing tomorrow: a comprehensive survey on the synergy of Artificial Intelligence and information security. AI and Ethics. 2025 Jun;5(3):1911-29. https://doi.org/10.1007/s43681-024-00529-z

[44] Jin F, Zhang X. Artificial intelligence or human: when and why consumers prefer AI recommendations. Information Technology & People. 2025 Jan 8;38(1):279-303. https://doi.org/10.1108/ITP-01-2023-0022

[45] Owan VJ, Abang KB, Idika DO, Etta EO, Bassey BA. Exploring the potential of artificial intelligence tools in educational measurement and assessment. Eurasia journal of mathematics, science and technology education. 2023 Aug 1;19(8):em2307. https://doi.org/10.29333/ejmste/13428

[46] Cukurova M. The interplay of learning, analytics and artificial intelligence in education: A vision for hybrid intelligence. British Journal of Educational Technology. 2025 Mar;56(2):469-88. https://doi.org/10.1111/bjet.13514

[47] Agha RA, Mathew G, Rashid R, Kerwan A, Al-Jabir A, Sohrabi C, Franchi T, Nicola M, Agha M. Transparency in the reporting of artificial intelligence-the TITAN guideline. Premier Journal of Science. 2025;10:100082. https://doi.org/10.70389/PJS.100082

[48] Hanna MG, Pantanowitz L, Dash R, Harrison JH, Deebajah M, Pantanowitz J, Rashidi HH. Future of artificial intelligence (AI)-machine learning (ML) trends in pathology and medicine. Modern Pathology. 2025 Jan 4:100705. https://doi.org/10.1016/j.modpat.2025.100705
[49] Chen E, Prakash S, Janapa Reddi V, Kim D, Rajpurkar P. A framework for integrating artificial intelligence for clinical care with continuous therapeutic monitoring. Nature Biomedical Engineering. 2025 Apr;9(4):445-54. https://doi.org/10.1038/s41551-023-01115-0
[50] Liu SY. Artificial intelligence (AI) in agriculture. IT professional. 2020 May 21;22(3):14-5. https://doi.org/10.1109/MITP.2020.2986121
[51] Shimizu H, Nakayama KI. Artificial intelligence in oncology. Cancer science. 2020 May;111(5):1452-60. https://doi.org/10.1111/cas.14377
[52] Schwendicke FA, Samek W, Krois J. Artificial intelligence in dentistry: chances and challenges. Journal of dental research. 2020 Jul;99(7):769-74. https://doi.org/10.1177/0022034520915714
[53] Verganti R, Vendraminelli L, Iansiti M. Innovation and design in the age of artificial intelligence. Journal of product innovation management. 2020 May;37(3):212-27. https://doi.org/10.1111/jpim.12523
[54] Novelli C, Taddeo M, Floridi L. Accountability in artificial intelligence: What it is and how it works. Ai & Society. 2024 Aug;39(4):1871-82. https://doi.org/10.1007/s00146-023-01635-y
[55] Rashidi HH, Pantanowitz J, Hanna MG, Tafti AP, Sanghani P, Buchinsky A, Fennell B, Deebajah M, Wheeler S, Pearce T, Abukhiran I. Introduction to artificial intelligence and machine learning in pathology and medicine: generative and nongenerative artificial intelligence basics. Modern Pathology. 2025 Apr 1;38(4):100688. https://doi.org/10.1016/j.modpat.2024.100688
[56] Waisberg E, Ong J, Kamran SA, Masalkhi M, Paladugu P, Zaman N, Lee AG, Tavakkoli A. Generative artificial intelligence in ophthalmology. Survey of ophthalmology. 2025 Jan 1;70(1):1-1. https://doi.org/10.1016/j.survophthal.2024.04.009
[57] Wang H, Fu T, Du Y, Gao W, Huang K, Liu Z, Chandak P, Liu S, Van Katwyk P, Deac A, Anandkumar A. Scientific discovery in the age of artificial intelligence. Nature. 2023 Aug 3;620(7972):47-60. https://doi.org/10.1038/s41586-023-06221-2
[58] Banh L, Strobel G. Generative artificial intelligence. Electronic Markets. 2023 Dec;33(1):63. https://doi.org/10.1007/s12525-023-00680-1
[59] Ahmed I, Jeon G, Piccialli F. From artificial intelligence to explainable artificial intelligence in industry 4.0: a survey on what, how, and where. IEEE transactions on industrial informatics. 2022 Jan 27;18(8):5031-42. https://doi.org/10.1109/TII.2022.3146552
[60] Alqahtani T, Badreldin HA, Alrashed M, Alshaya AI, Alghamdi SS, Bin Saleh K, Alowais SA, Alshaya OA, Rahman I, Al Yami MS, Albekairy AM. The emergent role of artificial intelligence, natural learning processing, and large language models in higher education and research. Research in social and administrative pharmacy. 2023 Aug 1;19(8):1236-42. https://doi.org/10.1016/j.sapharm.2023.05.016
[61] Bankins S, Formosa P. The ethical implications of artificial intelligence (AI) for meaningful work. Journal of Business Ethics. 2023 Jul;185(4):725-40. https://doi.org/10.1007/s10551-023-05339-7
[62] Abulibdeh A, Zaidan E, Abulibdeh R. Navigating the confluence of artificial intelligence and education for sustainable development in the era of industry 4.0: Challenges, opportunities, and ethical dimensions. Journal of Cleaner Production. 2024 Jan 15;437:140527. https://doi.org/10.1016/j.jclepro.2023.140527
[63] King MR, ChatGPT. A conversation on artificial intelligence, chatbots, and plagiarism in higher education. Cellular and molecular bioengineering. 2023 Feb;16(1):1-2. https://doi.org/10.1007/s12195-022-00754-8
[64] Ikhsan RB, Fernando Y, Prabowo H, Gui A, Kuncoro EA. An empirical study on the use of artificial intelligence in the banking sector of Indonesia by extending the TAM model and the moderating effect of perceived trust. Digital Business. 2025 Jun 1;5(1):100103. https://doi.org/10.1016/j.digbus.2024.100103
[65] Cui M, Zhang DY. Artificial intelligence and computational pathology. Laboratory Investigation. 2021 Apr 1;101(4):412-22. https://doi.org/10.1038/s41374-020-00514-0
[66] Messeri L, Crockett MJ. Artificial intelligence and illusions of understanding in scientific research. Nature. 2024 Mar 7;627(8002):49-58. https://doi.org/10.1038/s41586-024-07146-0
[67] Salvagno M, Taccone FS, Gerli AG. Can artificial intelligence help for scientific writing?. Critical care. 2023 Feb 25;27(1):75. https://doi.org/10.1186/s13054-023-04380-2
[68] Vasishta P, Dhingra N, Vasishta S. Application of artificial intelligence in libraries: a bibliometric analysis and visualisation of research activities. Library Hi Tech. 2025 May 19;43(2/3):693-710. https://doi.org/10.1108/LHT-12-2023-0589

[69] Samala AD, Rawas S, Wang T, Reed JM, Kim J, Howard NJ, Ertz M. Unveiling the landscape of generative artificial intelligence in education: a comprehensive taxonomy of applications, challenges, and future prospects. Education and Information Technologies. 2025 Feb;30(3):3239-78. https://doi.org/10.1007/s10639-024-12936-0

[70] Vora LK, Gholap AD, Jetha K, Thakur RR, Solanki HK, Chavda VP. Artificial intelligence in pharmaceutical technology and drug delivery design. Pharmaceutics. 2023 Jul 10;15(7):1916. https://doi.org/10.3390/pharmaceutics15071916

[71] Loureiro SM, Guerreiro J, Tussyadiah I. Artificial intelligence in business: State of the art and future research agenda. Journal of business research. 2021 May 1;129:911-26. https://doi.org/10.1016/j.jbusres.2020.11.001

[72] Najjar R. Redefining radiology: a review of artificial intelligence integration in medical imaging. Diagnostics. 2023 Aug 25;13(17):2760. https://doi.org/10.3390/diagnostics13172760

[73] Su J, Ng DT, Chu SK. Artificial intelligence (AI) literacy in early childhood education: The challenges and opportunities. Computers and Education: Artificial Intelligence. 2023 Jan 1;4:100124. https://doi.org/10.1016/j.caeai.2023.100124

[74] Soori M, Arezoo B, Dastres R. Artificial intelligence, machine learning and deep learning in advanced robotics, a review. Cognitive Robotics. 2023 Jan 1;3:54-70. https://doi.org/10.1016/j.cogr.2023.04.001

[75] Bhuyan SS, Sateesh V, Mukul N, Galvankar A, Mahmood A, Nauman M, Rai A, Bordoloi K, Basu U, Samuel J. Generative artificial intelligence use in healthcare: opportunities for clinical excellence and administrative efficiency. Journal of medical systems. 2025 Jan 16;49(1):10. https://doi.org/10.1007/s10916-024-02136-1

[76] Cooper G. Examining science education in ChatGPT: An exploratory study of generative artificial intelligence. Journal of science education and technology. 2023 Jun;32(3):444-52. https://doi.org/10.1007/s10956-023-10039-y

[77] Aldoseri A, Al-Khalifa KN, Hamouda AM. Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges. Applied Sciences. 2023 Jan;13(12):7082. https://doi.org/10.3390/app13127082

[78] George B, Wooden O. Managing the strategic transformation of higher education through artificial intelligence. Administrative Sciences. 2023 Aug 29;13(9):196. https://doi.org/10.3390/admsci13090196

[79] Wang B, Rau PL, Yuan T. Measuring user competence in using artificial intelligence: validity and reliability of artificial intelligence literacy scale. Behaviour & information technology. 2023 Jul 4;42(9):1324-37. https://doi.org/10.1080/0144929X.2022.2072768

[80] Morandini S, Fraboni F, De Angelis M, Puzzo G, Giusino D, Pietrantoni L. The impact of artificial intelligence on workers' skills: Upskilling and reskilling in organisations. Informing Science. 2023;26:39-68. https://doi.org/10.28945/5078

[81] Topaz M, Peltonen LM, Michalowski M, Stiglic G, Ronquillo C, Pruinelli L, Song J, O'connor S, Miyagawa S, Fukahori H. The ChatGPT effect: nursing education and generative artificial intelligence. Journal of Nursing Education. 2025 Jun 1;64(6):e40-3. https://doi.org/10.3928/01484834-20240126-01

[82] Noy S, Zhang W. Experimental evidence on the productivity effects of generative artificial intelligence. Science. 2023 Jul 14;381(6654):187-92. https://doi.org/10.1126/science.adh2586

[83] Nguyen A, Ngo HN, Hong Y, Dang B, Nguyen BP. Ethical principles for artificial intelligence in education. Education and information technologies. 2023 Apr;28(4):4221-41. https://doi.org/10.1007/s10639-022-11316-w

[84] Malatji M, Tolah A. Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. AI and Ethics. 2025 Apr;5(2):883-910. https://doi.org/10.1007/s43681-024-00427-4

[85] Shata A, Hartley K. Artificial intelligence and communication technologies in academia: faculty perceptions and the adoption of generative AI. International Journal of Educational Technology in Higher Education. 2025 Mar 14;22(1):14. https://doi.org/10.1186/s41239-025-00511-7

[86] Yuan L, Liu X. The effect of artificial intelligence tools on EFL learners' engagement, enjoyment, and motivation. Computers in Human Behavior. 2025 Jan 1;162:108474. https://doi.org/10.1016/j.chb.2024.108474

[87] Malhotra G, Ramalingam M. Perceived anthropomorphism and purchase intention using artificial intelligence technology: examining the moderated effect of trust. Journal of Enterprise Information Management. 2025 Feb 25;38(2):401-23. https://doi.org/10.1108/JEIM-09-2022-0316

[88] Abbasi BN, Wu Y, Luo Z. Exploring the impact of artificial intelligence on curriculum development in global higher education institutions. Education and Information Technologies. 2025 Jan;30(1):547-81. https://doi.org/10.1007/s10639-024-13113-z

[89] Baig MI, Yadegaridehkordi E. Factors influencing academic staff satisfaction and continuous usage of generative artificial intelligence (GenAI) in higher education. International Journal of Educational Technology in Higher Education. 2025 Feb 3;22(1):5. https://doi.org/10.1186/s41239-025-00506-4

[90] Bewersdorff A, Hartmann C, Hornberger M, Seßler K, Bannert M, Kasneci E, Kasneci G, Zhai X, Nerdel C. Taking the next step with generative artificial intelligence: The transformative role of multimodal large language models in science education. Learning and Individual Differences. 2025 Feb 1;118:102601. https://doi.org/10.1016/j.lindif.2024.102601

[91] Holzinger A, Keiblinger K, Holub P, Zatloukal K, Müller H. AI for life: Trends in artificial intelligence for biotechnology. New biotechnology. 2023 May 25;74:16-24. https://doi.org/10.1016/j.nbt.2023.02.001

[92] Kaplan A, Haenlein M. Rulers of the world, unite! The challenges and opportunities of artificial intelligence. Business horizons. 2020 Jan 1;63(1):37-50. https://doi.org/10.1016/j.bushor.2019.09.003

[93] Thiebes S, Lins S, Sunyaev A. Trustworthy artificial intelligence. Electronic Markets. 2021 Jun;31(2):447-64. https://doi.org/10.1007/s12525-020-00441-4

[94] Ullah F, Saqib S, Xiong YC. Integrating artificial intelligence in biodiversity conservation: bridging classical and modern approaches. Biodiversity and Conservation. 2025 Jan;34(1):45-65. https://doi.org/10.1007/s10531-024-02977-9

[95] An X, Chai CS, Li Y, Zhou Y, Yang B. Modeling students' perceptions of artificial intelligence assisted language learning. Computer Assisted Language Learning. 2025 Jul 4;38(5-6):987-1008. https://doi.org/10.1080/09588221.2023.2246519

[96] Crawford J, Cowling M, Allen KA. Leadership is needed for ethical ChatGPT: Character, assessment, and learning using artificial intelligence (AI). Journal of University Teaching and Learning Practice. 2023 Apr;20(3):1-9. https://doi.org/10.53761/1.20.3.02

[97] Naser MZ, Alavi AH. Error metrics and performance fitness indicators for artificial intelligence and machine learning in engineering and sciences. Architecture, Structures and Construction. 2023 Dec;3(4):499-517. https://doi.org/10.1007/s44150-021-00015-8

[98] Babina T, Fedyk A, He A, Hodson J. Artificial intelligence, firm growth, and product innovation. Journal of Financial Economics. 2024 Jan 1;151:103745. https://doi.org/10.1016/j.jfineco.2023.103745

[99] Alahi ME, Sukkuea A, Tina FW, Nag A, Kurdthongmee W, Suwannarat K, Mukhopadhyay SC. Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: recent advancements and future trends. Sensors. 2023 May 30;23(11):5206. https://doi.org/10.3390/s23115206

[100] Al Kuwaiti A, Nazer K, Al-Reedy A, Al-Shehri S, Al-Muhanna A, Subbarayalu AV, Al Muhanna D, Al-Muhanna FA. A review of the role of artificial intelligence in healthcare. Journal of personalized medicine. 2023 Jun 5;13(6):951. https://doi.org/10.3390/jpm13060951

[101] Ameen N, Tarhini A, Reppel A, Anand A. Customer experiences in the age of artificial intelligence. Computers in human behavior. 2021 Jan 1;114:106548. https://doi.org/10.1016/j.chb.2020.106548

[102] Hwang GJ, Chien SY. Definition, roles, and potential research issues of the metaverse in education: An artificial intelligence perspective. Computers and Education: Artificial Intelligence. 2022 Jan 1;3:100082. https://doi.org/10.1016/j.caeai.2022.100082

[103] Alier M, Peñalvo FJ, Camba JD. Generative Artificial Intelligence in Education: From Deceptive to Disruptive. International Journal of interactive multimedia and artificial intelligence. 2024 Mar 1;8(5):5-14. https://doi.org/10.9781/ijimai.2024.02.011

[104] Walter Y. Embracing the future of Artificial Intelligence in the classroom: the relevance of AI literacy, prompt engineering, and critical thinking in modern education. International Journal of Educational Technology in Higher Education. 2024 Feb 26;21(1):15. https://doi.org/10.1186/s41239-024-00448-3

[105] Chiu TK, Moorhouse BL, Chai CS, Ismailov M. Teacher support and student motivation to learn with Artificial Intelligence (AI) based chatbot. Interactive Learning Environments. 2024 Aug 8;32(7):3240-56.

[106] Cai H, Ao Z, Tian C, Wu Z, Liu H, Tchieu J, Gu M, Mackie K, Guo F. Brain organoid reservoir computing for artificial intelligence. Nature Electronics. 2023 Dec;6(12):1032-9. https://doi.org/10.1038/s41928-023-01069-w

[107] Jackson I, Ivanov D, Dolgui A, Namdar J. Generative artificial intelligence in supply chain and operations management: a capability-based framework for analysis and implementation. International Journal of Production Research. 2024 Sep 1;62(17):6120-45. https://doi.org/10.1080/00207543.2024.2309309

[108] Bibri SE, Krogstie J, Kaboli A, Alahi A. Smarter eco-cities and their leading-edge artificial intelligence of things solutions for environmental sustainability: A comprehensive systematic review. Environmental Science and Ecotechnology. 2024 May 1;19:100330. https://doi.org/10.1016/j.ese.2023.100330

[109] Sarraju A, Bruemmer D, Van Iterson E, Cho L, Rodriguez F, Laffin L. Appropriateness of cardiovascular disease prevention recommendations obtained from a popular online chat-based artificial intelligence model. Jama. 2023 Mar 14;329(10):842-4. https://doi.org/10.1001/jama.2023.1044

[110] Belhadi A, Mani V, Kamble SS, Khan SA, Verma S. Artificial intelligence-driven innovation for enhancing supply chain resilience and performance under the effect of supply chain dynamism: an empirical investigation. Annals of operations research. 2024 Feb;333(2):627-52. https://doi.org/10.1007/s10479-021-03956-x

[111] Gligorea I, Cioca M, Oancea R, Gorski AT, Gorski H, Tudorache P. Adaptive learning using artificial intelligence in e-learning: A literature review. Education Sciences. 2023 Dec 6;13(12):1216. https://doi.org/10.3390/educsci13121216

[112] Lee D, Yoon SN. Application of artificial intelligence-based technologies in the healthcare industry: Opportunities and challenges. International journal of environmental research and public health. 2021 Jan;18(1):271. https://doi.org/10.3390/ijerph18010271

[113] Anantrasirichai N, Bull D. Artificial intelligence in the creative industries: a review. Artificial intelligence review. 2022 Jan;55(1):589-656. https://doi.org/10.1007/s10462-021-10039-7

[114] Haug CJ, Drazen JM. Artificial intelligence and machine learning in clinical medicine, 2023. New England Journal of Medicine. 2023 Mar 30;388(13):1201-8. https://doi.org/10.1056/NEJMra2302038

[115] Krakowski S, Luger J, Raisch S. Artificial intelligence and the changing sources of competitive advantage. Strategic Management Journal. 2023 Jun;44(6):1425-52. https://doi.org/10.1002/smj.3387

[116] Abioye SO, Oyedele LO, Akanbi L, Ajayi A, Delgado JM, Bilal M, Akinade OO, Ahmed A. Artificial intelligence in the construction industry: A review of present status, opportunities and future challenges. Journal of Building Engineering. 2021 Dec 1;44:103299. https://doi.org/10.1016/j.jobe.2021.103299

[117] Aung YY, Wong DC, Ting DS. The promise of artificial intelligence: a review of the opportunities and challenges of artificial intelligence in healthcare. British medical bulletin. 2021 Sep;139(1):4-15. https://doi.org/10.1093/bmb/ldab016

[118] Kousha K, Thelwall M. Artificial intelligence to support publishing and peer review: A summary and review. Learned Publishing. 2024 Jan;37(1):4-12. https://doi.org/10.1002/leap.1570

[119] Gangwal A, Lavecchia A. Artificial intelligence in natural product drug discovery: current applications and future perspectives. Journal of medicinal chemistry. 2025 Feb 7;68(4):3948-69. https://doi.org/10.1021/acs.jmedchem.4c01257

[120] Crompton H, Burke D. Artificial intelligence in higher education: the state of the field. International journal of educational technology in higher education. 2023 Apr 24;20(1):22. https://doi.org/10.1186/s41239-023-00392-8

[121] Puntoni S, Reczek RW, Giesler M, Botti S. Consumers and artificial intelligence: An experiential perspective. Journal of marketing. 2021 Jan;85(1):131-51. https://doi.org/10.1177/0022242920953847

[122] Kumar I, Rawat J, Mohd N, Husain S. Opportunities of artificial intelligence and machine learning in the food industry. Journal of Food Quality. 2021;2021(1):4535567. https://doi.org/10.1155/2021/4535567

[123] Moor M, Banerjee O, Abad ZS, Krumholz HM, Leskovec J, Topol EJ, Rajpurkar P. Foundation models for generalist medical artificial intelligence. Nature. 2023 Apr 13;616(7956):259-65. https://doi.org/10.1038/s41586-023-05881-4

[124] Jaiswal A, Arun CJ, Varma A. Rebooting employees: Upskilling for artificial intelligence in multinational corporations. InArtificial intelligence and international HRM 2023 May 22 (pp. 114-143). Routledge. https://doi.org/10.4324/9781003377085-5

[125] Nie J, Jiang J, Li Y, Wang H, Ercisli S, Lv L. Data and domain knowledge dual-driven artificial intelligence: Survey, applications, and challenges. Expert Systems. 2025 Jan;42(1):e13425. https://doi.org/10.1111/exsy.13425

[126] Nenni ME, De Felice F, De Luca C, Forcina A. How artificial intelligence will transform project management in the age of digitization: a systematic literature review. Management Review Quarterly. 2025 Jun;75(2):1669-716. https://doi.org/10.1007/s11301-024-00418-z

[127] Qin C, Zhang L, Cheng Y, Zha R, Shen D, Zhang Q, Chen X, Sun Y, Zhu C, Zhu H, Xiong H. A comprehensive survey of artificial intelligence techniques for talent analytics. Proceedings of the IEEE. 2025 Jun 6. https://doi.org/10.1109/JPROC.2025.3572744

[128] Kaack LH, Donti PL, Strubell E, Kamiya G, Creutzig F, Rolnick D. Aligning artificial intelligence with climate change mitigation. Nature Climate Change. 2022 Jun;12(6):518-27. https://doi.org/10.1038/s41558-022-01377-7

[129] Ali S, Abuhmed T, El-Sappagh S, Muhammad K, Alonso-Moral JM, Confalonieri R, Guidotti R, Del Ser J, Díaz-Rodríguez N, Herrera F. Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence. Information fusion. 2023 Nov 1;99:101805. https://doi.org/10.1016/j.inffus.2023.101805

[130] Kelly S, Kaye SA, Oviedo-Trespalacios O. What factors contribute to the acceptance of artificial intelligence? A systematic review. Telematics and informatics. 2023 Feb 1;77:101925. https://doi.org/10.1016/j.tele.2022.101925

[131] Bhattamisra SK, Banerjee P, Gupta P, Mayuren J, Patra S, Candasamy M. Artificial intelligence in pharmaceutical and healthcare research. Big Data and Cognitive Computing. 2023 Jan 11;7(1):10. https://doi.org/10.3390/bdcc7010010

[132] Pallathadka H, Ramirez-Asis EH, Loli-Poma TP, Kaliyaperumal K, Ventayen RJ, Naved M. Applications of artificial intelligence in business management, e-commerce and finance. Materials Today: Proceedings. 2023 Jan 1;80:2610-3. https://doi.org/10.1016/j.matpr.2021.06.419

[133] McDonald N, Johri A, Ali A, Collier AH. Generative artificial intelligence in higher education: Evidence from an analysis of institutional policies and guidelines. Computers in Human Behavior: Artificial Humans. 2025 Mar 1;3:100121. https://doi.org/10.1016/j.chbah.2025.100121

[134] Emon MM, Khan T. The mediating role of attitude towards the technology in shaping artificial intelligence usage among professionals. Telematics and Informatics Reports. 2025 Mar 1;17:100188. https://doi.org/10.1016/j.teler.2025.100188

[135] Shao X, Cai B, Zou Z, Shao H, Yang C, Liu Y. Artificial intelligence enhanced fault prediction with industrial incomplete information. Mechanical Systems and Signal Processing. 2025 Feb 1;224:112063. https://doi.org/10.1016/j.ymssp.2024.112063

[136] Rožanec JM, Novalija I, Zajec P, Kenda K, Tavakoli Ghinani H, Suh S, Bian S, Veliou E, Papamartzivanos D, Giannetsos T, Menesidou SA. Human-centric artificial intelligence architecture for industry 5.0 applications. International journal of production research. 2023 Oct 18;61(20):6847-72. https://doi.org/10.1080/00207543.2022.2138611

[137] Chander B, John C, Warrier L, Gopalakrishnan K. Toward trustworthy artificial intelligence (TAI) in the context of explainability and robustness. ACM Computing Surveys. 2025 Feb 10;57(6):1-49. https://doi.org/10.1145/3675392

[138] Horani OM, Al-Adwan AS, Yaseen H, Hmoud H, Al-Rahmi WM, Alkhalifah A. The critical determinants impacting artificial intelligence adoption at the organizational level. Information Development. 2025 Sep;41(3):1055-79. https://doi.org/10.1177/02666669231166889

[139] Varriale V, Cammarano A, Michelino F, Caputo M. Critical analysis of the impact of artificial intelligence integration with cutting-edge technologies for production systems. Journal of Intelligent Manufacturing. 2025 Jan;36(1):61-93. https://doi.org/10.1007/s10845-023-02244-8

[140] Fu C, Chen Q. The future of pharmaceuticals: Artificial intelligence in drug discovery and development. Journal of Pharmaceutical Analysis. 2025 Feb 26:101248. https://doi.org/10.1016/j.jpha.2025.101248