INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Advancing Smart Industries with Internet of Things and Artificial Intelligence: A Digital Ecosystem Perspective

Asmarani Ahmad Puzi, Ahmad Anwar Zainuddin*, Muhammad Afham Anuar, Muhammad Farees Afandi & Ahmad Fatzilah Misman
Kulliyyah of Information and Communication Technology
International Islamic University Malaysia (IIUM)
Kuala Lumpur, Malaysia
Email: asmarani@iium.edu.my; *anwarzain@iium.edu.my; anwarzain@iium.edu.my; fareesafandi05@gmail.com ; afatzilah@iium.edu.my

Saidatul Izyanie Kamarudin
Fakulti Sains Komputer & Matematik
Universiti Teknologi MARA (UiTM)
Kuala Lumpur, Malaysia
Email: saidatulizyanie@uitm.edu.my

Submitted: 15/9/2025. Revised edition: 28/11/2025. Accepted: 5/1/2026. Published online: 28/7/2026
DOI: https://doi.org/10.11113/ijic.v16n1-2.693

***Abstract*—The digital transformation of industrial systems under the Industry 4.0 paradigm has introduced cyber-physical systems (CPS) as a core enabler of vertical integration and data-driven production environments. The convergence of Internet of Things (IoT) and Artificial Intelligence (AI) technologies has accelerated this transformation, fostering the development of the Industrial Internet of Things (IIoT) and creating smart industries characterized by real-time monitoring, automation, and human–robot collaboration (HRC). While these advancements establish a digital ecosystem capable of optimizing production through intelligent data analysis and decision-making, their practical implementation remains constrained by unresolved challenges and gaps in validation. With the emergence of Industry 5.0, the focus shifts toward human-centric, sustainable, and resilient industrial ecosystems, where AI-driven cognitive computing further enhances interaction between humans and machines. This review examines the application of AI–IoT integrated technologies across multiple industrial domains to identify their strengths, limitations, and recurring challenges. By categorizing existing literature into key application areas, the study highlights both the opportunities and risks inherent in current approaches, bridging the conceptual design of smart industries with their real-world realizations. The findings underscore the importance of scalable, secure, and efficient frameworks to ensure the safe and reliable adoption of AI–IoT in the industrial ecosystem.**

***Keywords*—Internet of Things, Artificial Intelligence, Smart Industry, Optimization**

I. INTRODUCTION

All The digital transformation has realized the adoption of Industry 4.0, its advantage is mainly in the ability to reform the value chain of industry with the integration of cyber-physical systems (CPS), which enabled vertical integration with networked industrial systems [1]. The core of Industry 4.0 is the integration of CPS into the value chain, allowing digital control over physical processes in the production lifecycle by leveraging Internet of Things (IoT) technologies that are interconnected via software and protocols. This integration defined the formulation of the Industrial Internet of Things (IIoT), which enabled real-time movement of data for automation and guidance in production environments [2]. The advent of smart industry is possible through an integrated ecosystem of interconnected devices, monitoring, adjusting, and maintaining industrial machines while closely working with humans in a shared environment through human–robot collaboration (HRC) [30], creating a symbiotic digital ecosystem. The fourth industrial revolution has brought forth the integration of smart technologies within the industrial environment [3].

With recent advancements in artificial intelligence, its integration within industrial systems is inevitable, as it enables cognitive computing capabilities that transform the automation of industrial processes through optimized procurement and analysis of quality data [4]. The advent of cognitive computing improves human–computer interaction through its ability to mimic human decision-making via speech processing, natural language processing, and machine learning [4]. The integration and transformation of industry into a data-driven production system represent an evolution of Industry 4.0 toward more efficient and meaningful human–machine collaboration, with AI as a core component promoting a more human-centric, sustainable, and resilient industry, referred to as Industry 5.0 [3].

However, the practical implementation of Industry 5.0 remains vague and lacks real-world validation. Despite this, the integration of AI and IoT is fundamental to this innovation, where improvements within the digital ecosystem are expected to bridge the gap between conceptual design and practical realization. Across the AI–IoT integration paradigm, the pace of advancement is rapid, with various industries seeking to improve production and industrial systems by adopting this paradigm as a primary strategy. Numerous AI–IoT-integrated applications in smart industries aim to address these demands; however, their limitations and gaps remain uncertain. Fig. 1 illustrates the general implementation of AI–IoT-integrated systems in smart industries.

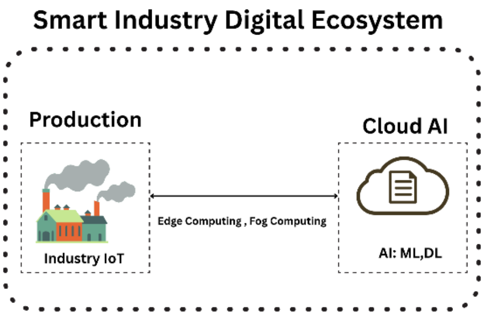


Fig. 1. Integration of IoT and AI in Smart Industry through Edge and Fog Computing

This review aims to provide the application of AI and IoT integrated technologies within smart industries, as an outcome we will address the recurring problem of an application which will be categorized in domains for better understanding. This paper will be outlined as follows; section I will give a brief overview of IoT, AI as digital ecosystem and smart industry. Section II will summarize the literature review that is included in this work. Section III disclose the methodology that is used throughout the research process of this paper. Section IV presents a discussion and improvement in the various aspects and industries encompassing the paradigm.

II. Literature Review

The industrial digital ecosystem has been reshaped by the integration of Artificial Intelligence (AI) and the Internet of Things (IoT), with applications across a variety of technologies that have driven the evolution of Industry 4.0 and its transition toward Industry 5.0. Bolbotinović *et al.* [5] proposed a multivariate time-series forecasting method for optimizing energy processes through the fusion of Digital Twin (DT) models with vertically integrated IoT systems and advanced machine learning (ML) techniques deployed via fog and edge computing. This approach enables real-time synchronization between physical and digital systems, improving parameter tuning, operational efficiency, and maintenance optimization. Similarly, Reyes-Acosta *et al.* [6] demonstrated a machine learning (ML) and deep learning (DL)-driven Intrusion Detection System (IDS) designed to deter dynamic threats, despite challenges related to computational resource limitations, data quality, and device heterogeneity. In parallel, Abdulrazzq *et al.* [7] introduced an AI-based predictive maintenance system employing decision trees, random forests, and recurrent neural networks, which enhances the reliability of IoT operations through significant reductions in system downtime and maintenance costs compared to traditional approaches.

In the context of energy management, Romero and Recto [8] simulated an IoT-driven hybrid microgrid using intelligent actuators and sensors for energy allocation. Although the validation remains purely simulated, the study reveals potential improvements in energy efficiency and carbon reduction. In Architecture, Engineering, and Construction (AEC) applications, Rane *et al.* [9] proposed AI- and IoT-based sensor systems as key enablers of predictive decision-making and risk mitigation throughout the project lifecycle, although implementation remains constrained by infrastructure readiness and workforce limitations.

Multiple sectors, including healthcare, finance, and transportation, have been transformed by the integration of AI, IoT, and big data through interconnected ecosystems and accelerated development cycles. However, this innovation has rapidly outpaced the availability of skilled labor [10]. In agriculture, Thotho and Macheso [11] introduced precision agriculture practices through real-time monitoring and automated decision-making for crop, livestock, and soil management using AI, IoT, and ML. These practices were further enhanced by Ayall *et al.* [12], who employed IoT-based environmental sensing and AI-driven backcasting methods combining synthetic and real data to improve yield forecasting accuracy in strawberry production.

Despite these advances, security challenges persist. Feng *et al.* [13] highlighted vulnerabilities in IoT communication networks that can be exploited through interference attacks, recommending improved encryption techniques and multi-signal protection strategies. Addressing cybersecurity concerns in Industrial IoT (IIoT), Al Rawajbeh *et al.* [14] proposed an adaptive AI-based IDS incorporating Shapley Additive Explanations (SHAP) to enhance detection explainability. The system demonstrated high accuracy and adaptability in edge computing environments, despite limitations related to processing overhead and dataset dependence. Similarly, Imran *et al.* [15] examined the integration of Software-Defined Networking (SDN) with IoT using ML-based solutions to improve optimization, automation, and fault tolerance, although challenges related to resource allocation and interoperability remain unresolved. Rajavel *et al.* [16] further developed an IoT-based smart healthcare surveillance system, known as the Cloud-based Object Tracking and Behavior Identification System (COTBIS), which integrates DL for fall detection and edge computing to reduce bandwidth and latency, though its deployment is constrained by distance limitations.

For energy and workload optimization, Demirbaga [17] introduced a task scheduling mechanism using Ant Colony Optimization (ACO) and Multilayer Perceptron (MLP) neural networks to improve energy and carbon efficiency in IIoT-enabled cloud environments. This approach demonstrated intelligent power consumption management and workload distribution. Additionally, Alsuwaelim [18] emphasized intelligent AI and ML strategies for multi-layered cybersecurity in AI-based IoT networks, focusing on perception, network, and application layers to enhance anomaly detection and encryption, despite the inherent risks of algorithmic bias.

In the healthcare domain, the convergence of AI and IoT has transformed medical systems into predictive and personalized ecosystems. Popov *et al.* [19] demonstrated that continuous patient data streams collected via IoT sensors and analyzed using big data analytics (BDA) enable proactive health monitoring and more efficient hospital management. Similarly, Paul *et al.* [20] illustrated how AI–IoT integration within secure cloud-based frameworks using deep learning and neuro-fuzzy models has advanced neuroscience research and remote patient monitoring. This development was extended by Chen *et al.* [21], who introduced a Human Digital Twin (HDT) system supported by generative AI (GAI) to model physiological and psychological attributes, thereby improving diagnostic accuracy and patient care efficiency. Mwanza *et al.* [22] further explored AI–IoT applications in low- and middle-income countries (LMICs), highlighting scalable telemedicine and diagnostic support while noting limitations in connectivity, infrastructure, and standardization.

From an algorithmic perspective, Khan *et al.* [4] proposed a distributed federated learning (DFL) framework to optimize resource allocation and enhance robustness in cognitive IoT systems. Building on this paradigm, Singh *et al.* [24] developed a federated learning-based multi-objective optimization algorithm to improve distributed computation efficiency and data privacy across IoT devices. Collectively, these studies demonstrate that AI–IoT convergence is shaping modern industry, agriculture, and healthcare by enabling intelligent, data-driven ecosystems that enhance efficiency, prediction, and sustainability, while continuing to face challenges related to scalability, cybersecurity, and real-world deployment.

III. Methodology

This reviews adopts a structure consist combination of literature synthesis and survey analysis. The literature is collected through academic sources via Google Scholar, Emerald Insight and Springer. For reliability reference, the papers are chosen between the years 2020 and 2025, reflecting the recent updates on AI-IoT integration, which is still new in this era. The survey includes a total of 30 random persons in public society, avoiding bias results.

The study literature reviews are chosen with several factors (i) examined in the contents that talk solely on AI-IoT integration and are related to key words: 'AI', 'IoT', 'healthcare', 'agriculture', 'security' and 'smart industry'. (ii) The papers that mention only AI or IoT without integration or only introduce its basic concepts are excluded.

During the full text analysis, a theme forming up consists of 5 key domains that apply and adapt well to AI-IoT integration; Cybersecurity, Industrial Optimization, Healthcare, Agriculture, and Algorithms. These domains represent vertical industry-specific applications while having horizontal enabler functions. Through the study, the content is highlighted on their objective, methods and clear results while also identifying their strengths and limitations. This gives the key for arguments and true evidence mapped out to be further compared with survey analysis.

IV. Result and Discussion

The combination of IoT and AI in the smart industry gives significant advancements in productivity, maintainability, and sustainability. This paradigm can benefit any industry by introducing innovation to production processes. However, several issues need to be addressed for it to operate effectively and produce beneficial output. The paradigm can be categorized into various aspects and industries to address these improvements. Fig. 2 illustrates key areas where technology innovation has significantly contributed.

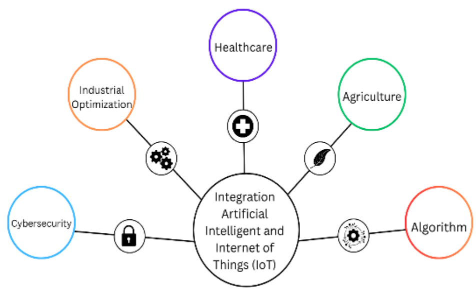


Fig. 2. Visualization of integration of AI and IoT covered in paper

A. Cybersecurity

Cybersecurity is a critical aspect that needs to be addressed in IoT and AI integration in the smart industry system, as it poses a risk of security vulnerability, confidentiality and availability of data and IoT systems. Based on Fig. 4E, the integration of AI-IoT carries a high risk in the cybersecurity field, as it is something virtual. Reyes-Acosta *et al.* [6] highlight that cybersecurity will encounter formidable challenges requiring meticulous attention, preparation of countermeasures, and strategic mitigation. It points out the use of IDS as an AI-driven tech to improve the IIoT ecosystems. Fig. 4H pointed out that the majority of the public agrees that data privacy and security carry a hard challenge to adopt within AI-IoT. Feng *et al.* [13] focus on communication security through IoT-driven digital twins, improving data sharing and its security through the emphasis of physical-layer interference tracking such as Catch the Jammer (CJ) algorithm. The purpose is to disturb the node set, making it complicated to be exposed to cyber threats. Alsuwaelim [18] compiles the latest cyber threats in the scope of AI-IoT connection through deep analysis of research papers while also finding each of its solutions. Most of the AI functions are to detect the risks and threats, but some of the mitigation is able to be solved by AI itself via IDS, such as authentication and data encryption. Similarly, Mishra [25] demonstrates that AI-driven DL and ML are able to give constant yet higher accuracy in identifying the emerging threats while also providing adaptive solutions compared to traditional methods. In a more recent study, Al Rawajbeh *et al*. [14] propose an adaptive IDS that combines online learning with explainable AI methods like SHAP. Their system improves accuracy but, more importantly, makes the decisions transparent enough for operators to understand. Taken together, these studies show that IDS in IIoT should be designed to adapt, explain their reasoning, and still run efficiently so that security can keep up with fast-changing industrial threats.

Figure 3 shows the simple implementation of the general IDS system; the monitor represents a general end device, and the diagram is intended to illustrate the interconnection of devices within the environment IDS is aware of.

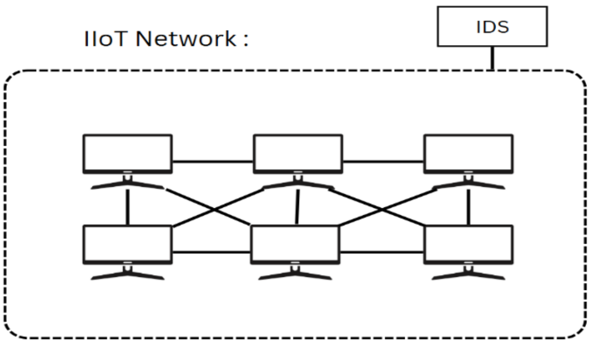


Fig. 3. Example of simple network-based IDS (NIDS)

A. Industrial Optimization

Industrial optimization remains the primary benefit of the smart industry. Within the studied literature of AI and IoT integration it has enabled real-time decision making, predictive maintenance and improvement of energy efficiency. Bolbotinović *et al*. [5] presented an integration of the DT model in industrial IoT, while utilizing ML algorithms for industrial energy processes by synchronizing virtual models and physical processes which enabled real-time parameter tuning and increases in efficient maintenance. Rane *et al*. [9] emphasize the reduction of cost and mitigation of risk across the project lifecycle in AEC sectors by employing AI- and IoT-based sensors which exhibit novel predictive capabilities. However, security, interoperability, skills gaps and scalability remains a concern for its successful implementation. Ayall *et al*. [12] provide a practical implementation of strawberry yield forecasting by employing IoT-based sensors in the production polytunnels and AI-driven backcasting to generate synthetic data and combining it with real data to outperform crop forecasting models that rely solely on real dataset. In parallel, Abdulrazzq *et al*. [7] demonstrated AI contribution to operational efficiency in significant reduction of downtime and maintenance cost using AI-driven predictive maintenance that implemented decision trees, random forests and recurrent neural networks compared to traditional methods. Imran *et al*. [26] explore the aspect of networking in the application of machine learning in SDN to improve the security, optimization and automation of IoT networks, while also highlighting its challenges such as interoperability, poor resource allocation and standardized tools. Finally, Romero and Recto [8] propose a design of hybrid microgrid system that integrates IoT-enabled sensor, automation system and intelligent actuator for energy optimization and carbon reduction in industrial systems. However, it is primarily a simulation and a practical implementation is yet to be explored.

Collectively, the application of AI and IoT integrated in the domain of industrial optimization offer a common trade-off: (1) advanced application requires high cost. From the application of digital twin and predictive maintenance that offer a high performance, both of these applications necessitates the usage of high and consistent energy, robust infrastructure and large dataset for AI to operate properly. (2) simulated and conceptual applications lack practical validation. The implementation of conceptual base models like hybrid micro-grid systems, still exhibits unknown costs, scalability and real world adoption. This concern is reflected in our perception survey, in which (according to Figure 4H) 27.59% of respondents agree with high implementation cost as being the main challenge in the implementation of AI and IoT integrated technology.

The findings from the convergence of both academic literature and perception survey highlights the need for standardized, scalable and affordable solutions for the future work that integrate both AI and IoT in its application.

B. Healthcare

Healthcare is being reshaped by the convergence of AI and IoT, discovering the potential of innovative improvement in medical care for prevention, diagnosis, treatment and management of illness This integration, often termed the Artificial Intelligence of Things (AIoT) or Healthcare IoT (H-IoT), is transforming the sector into a predictive and personalized system [19]. Research demonstrates substantial perceived improvements in operational efficiency, with surveys in Figure 4B showing that 41.38% of respondents reported extremely improved efficiency, 27.59% very much improved, 27.59% moderately improved, and 3.45% slightly improved, indicating strong positive reception of these technologies in healthcare settings.

These efficiency gains manifest across various applications. Systems like COTBIS enable real-time fall detection using edge computing to reduce bandwidth and latency, as demonstrated by Rajavel *et al*. [16]. Similarly, Chen *et al*. [21] show how Human Digital Twins (HDTs) leverage generative AI for personalized, continuous health monitoring by overcoming traditional limitations like high cost and poor data quality. Ghatge and Parasar [10] further recognize the broader potential for data-driven growth in the sector through advanced device connectivity.

The integration creates an intelligent ecosystem where continuous streams of patient data from IoT sensors are analyzed by AI algorithms, enabling proactive health monitoring, early disease detection, and optimized resource management [19]. This synergy is particularly transformative for Healthcare 4.0, where IoT devices collect real-time physiological data that AI transforms into actionable knowledge and predictive diagnostics [20]. The application extends to low- and middle-income countries (LMICs), where this technology helps overcome systemic barriers by enabling remote healthcare delivery and enhancing diagnostic precision [22].

However, despite these efficiency improvements, significant barriers impede widespread adoption. Ghatge and Parasar [10] highlight a major human capital gap, where rapid technological advancement outpaces the development of a skilled workforce capable of managing these systems. Chen et al. [21] further emphasize the critical infrastructure requirements, such as reliable high-bandwidth connectivity for data-intensive applications like HDTs. A particularly critical limitation is the severe vulnerability to data privacy breaches and cyberattacks [19]. The sensitive nature of continuously collected health data makes it a prime target, and securing a vast network of IoT devices presents a major challenge that requires meticulous attention to security protocols [20], [19]. Furthermore, the system's effectiveness is limited by its reliance on accurate sensor data and the potential for AI algorithms to perpetuate biases if trained on flawed datasets [19]. In LMICs, additional challenges include inconsistent internet connectivity, power reliability issues, and a scarcity of technical expertise for implementation and maintenance [22].

The primary hurdle is therefore no longer technical feasibility but the "last mile" of deployment, requiring coordinated investment in training, infrastructure, and security to translate prototypes and efficiency gains into practical, equitable clinical solutions across diverse healthcare environments.

C. Agriculture

The agricultural sector is experiencing rapid advancement with the integration of AI, ML, and IoT. Thotho and Macheso [11] demonstrated a model of precision agriculture to enable data-driven decision making for crop, live-stock and soil management. These integration of technologies has enhanced the productivity, reduced risk and increased sustainability of farming processes. In the aspect of crop management, Thotho and Macheso [11] has optimised the production of farmers by utilizing ML techniques such as yield forecasting, disease identification and weed detection. Additionally, the soil sensors and IoT-enabled livestock monitoring system provide real-time data to enhance feeding strategies, irrigation and fertilisation.

The efficiency of agriculture can also be optimized using smart sensing technologies which can help overcome issues caused by climate changes, resource scarcity and labour shortages. Miller *et al*. [27] proposed a precision irrigation and fertilisation that are enabled by IoT sensor networks and AI-driven analytics, though it lacks basic encryption network protocols, which raised concern about cybersecurity. Adli *et al*. [28] improved crop yield and efficiency through AI-IoT deep learning application such as Convolutional Neural Network (CNN) and Mask Regional-based Convolutional Neural Network (R-CNN) based models for early disease detection, robotic harvesters and predictive irrigation systems but require high cost of deployment and connectivity. Ibrahim *et al*. [29] proposed low-cost systems using Raspberry Pi and edge-based plant disease detection show promising results in terms of accuracy. However, it’s still require improvement to overcome challenges from environmental variability and unstable connections in rural farming areas. Moreover, lightweight AI models such as MobileNet and TinyML and IoT-edge systems such as LoRaWAN and ZigBee are able to provide fast and localised insights in resource-limited areas Abhishek *et al*. [30].

Survey findings also indicate support for the integration of AI and IoT in agriculture. Respondents recognized cybersecurity risks and data privacy as the most critical challenges in Fig. 4E and Fig. 4H, while 48.28% expressed confidence in the reliability of AI and IoT systems (Fig. 4F). In the agriculture aspect, these responses reveal the importance of developing a secure and trustworthy systems for farming data, ensuring disease detection, and maintaining consistent operation in rural and resource-limited farming environments is equally required.

In general, the application of AI and IoT in the agricultural sector not only increases efficiency but also introduces critical safety challenges. Addressing these challenges requires stronger cybersecurity protocols and reliable datasets for AI model training, which are essential to ensure trustworthy adoption by the sector.

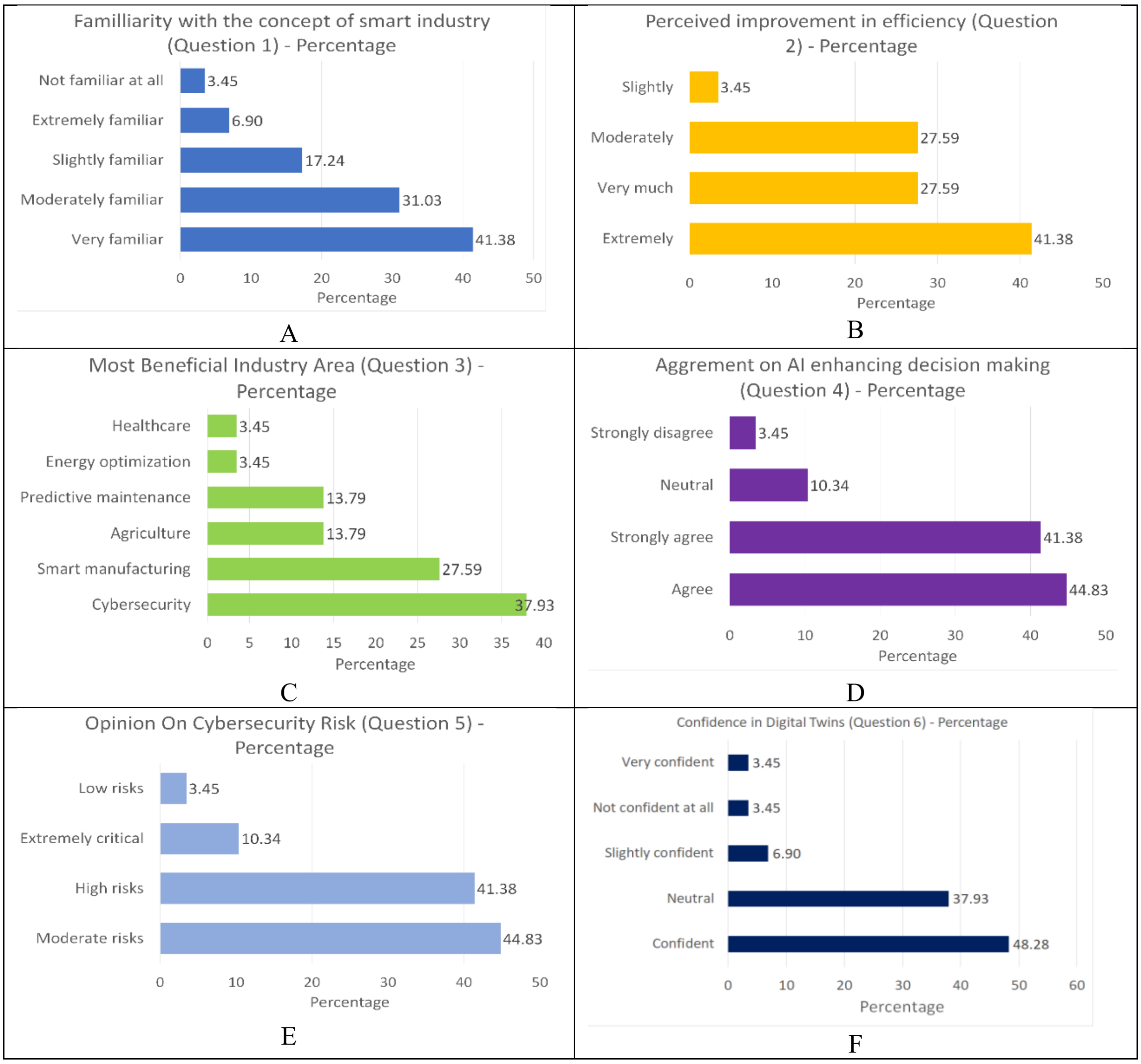
D. Algorithm

Algorithms design remain as the primary enabler of AI and IoT integration, ensuring its security, efficiency and sustainability. Its adoption defined AI intelligence and implementation it offers. Demirbaga [17] proposed an intelligent task scheduling mechanism utilizing predictive capability of MLP neural network and ACO algorithm to forecast energy consumption and balance workload in IIoT cloud environment. Through adaptive scheduling, this approach provides a solution for managing energy use, although it’s dependent on accuracy of prediction models and quality of input data. Decentralized network of IIoT is addressed by Sasikumar *et al*. [32] for its concern on reliability and security, the paper proposed an improved Delegated Proof of Stake (DPoS) consensus algorithm to increase the transaction speed and privacy of IIoT networks while also reducing energy consumption by leveraging an honor voting system in a creation of decentralized ledger. In contrast, Sujatha *et al*. [33] present a lightweight solution in optimizing IIoT systems by implementing a machine-learning technique using decision trees for data classification and anomaly detection. As an outcome, the technique improved the efficiency of the IIoT system to 78%, although the performance is dependent on the full production chain.

FL is also explored as an emerging paradigm of algorithm design, offering privacy in AI-IoT integrated systems. Khan *et al*. [4] introduces a novel DFL framework that improves the security, robustness and resource optimization of C-IoT, while also formulating an integer linear optimization problem to minimize FL cost for this framework. Comparing it with standard FL models, this scheme is proven to outperform it. Singh *et al*. [24] extend this paradigm by implementing another novel federated learning-based multi-objective optimization (FL-MOO), which primarily performs well for monitoring use cases of massive data from consumer end devices. This improvement of FL utilized a distributed IoT to balance computational load and maintain the accuracy of data. Both studies highlight the potential of large-scale, distributed AI and IoT integration to ensure data privacy and AI operational efficiency enabled by FL, despite there being a common trade off of computational efficiency and communication overhead.

Altogether, the studied literature illustrates a fragmented innovation encompassing algorithmic design for industrial IoT. Intelligent task scheduling and consensus mechanisms improve efficiency and security which is also aligned with public perception from our survey, in which (according to Figure 4B) 41.38% of respondents express AI and IoT integration to extremely improve the efficiency of the smart industry. Anomaly detection and federated learning address scalability and data integrity, which is important considering the result of our survey, in Figure 4D, where 44.38% of respondents agree with AI to improve decision making. Thus emphasising the importance of a reliable algorithmic model. However, there are persisting recurring challenges: (1) dependence on domain-specific dataset, (2) scalability to heterogeneous and resource constrained industrial environment and (3) lack of validation beyond controlled experiments.

By converging academic literature and public perception, the outcome suggests that future work must move toward an integrated framework that combines efficiency, security and scalability in algorithmic design, rather than isolated processes and experiments. Doing so will bridge the gap between advanced and costly methods and lightweight, limited solutions for safety and reliability of algorithm deployment in the real life smart industry ecosystem.



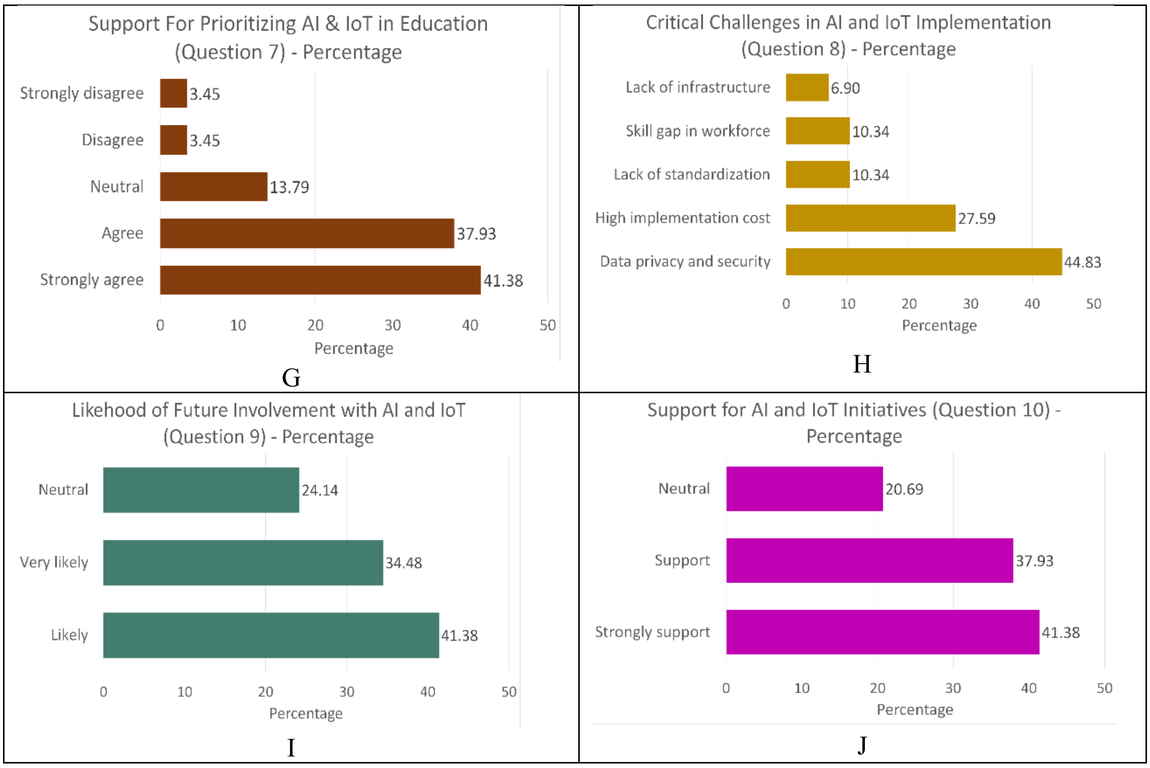


Fig. 4. These bar charts present the collection of responses to a survey titled "Perception towards Internet of Things and Artificial Intelligence in Smart Industry"

V. CONCLUSION

In summary, the integration of AI and IoT has the potential to innovate and progress the industry 4.0 and support the transition to industry 5.0 by its smart, intelligent and automatic capabilities in industrial application. Despite that, challenges remain persistent in the process of innovation and changes such as security, reliability, feasibility and scalability of a system that implemented this paradigm. This paper introduced a categorized application of AI and IoT integration in smart industries, with a focus on horizontal enablers such as cybersecurity, industrial optimization and agriculture and vertical application such as healthcare and agriculture of these technologies. The conducted qualitative study that combines literature review and perception survey reveals the benefits and challenges of the application of AI and IoT and reflects on its potential implementation. The study finds that there is a consistent practice of securing the AI and IoT integrated technologies which utilized IDS to leverage its capabilities of wide device coverage, the potential cost and lack of practical real-life validation in the conception of industrial optimized AI-IoT integrated system and a potential of predictive and personalized system for the application of AI-IoT technologies in healthcare, however there is still a lack of skilled labour, infrastructure and system security for proper implementation. In the agriculture sector, AI-IoT integrated technology improved automation, sustainability and productivity of farming processes. Although, to ensure a proper practical implementation it still needs proper cybersecurity protocols and reliable dataset. Lastly, algorithm is the enabler of AI and IoT integrated technology by ensuring security, efficiency and sustainability of the systems. However, the algorithm design should move towards and integrated framework that combine efficiency, security and scalability for proper adoption in AI and IoT integrated system in smart industries.

ACKNOWLEDGMENT

We would like to express our gratitude to all who have contributed to succeeding in this research. Special thanks to our instructor for the guidance along our journey in this research. Their unwavering commitment has greatly contributed to our advancement, enhancing our skills and deepening our understanding of enhancing network topologies, security challenges, and OSI model adaptation. In addition, thanks to KICT and IoTeams for allowing this work to be published.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

REFERENCES

[1] Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. *Information Systems Frontiers, 27*(1), 215–234. https://doi.org/10.1007/s10796-021-10221-w

[2] Radanliev, P., De Roure, D., Nicolescu, R., Huth, M., & Santos, O. (2021). Artificial intelligence and the Internet of Things in Industry 4.0. *CCF Transactions on Pervasive Computing and Interaction, 3*(3), 329–338. https://doi.org/10.1007/s42486-021-00057-3

[3] Zalozhnev, A. Y., & Ginz, V. N. (2023). Industry 4.0: Underlying technologies. Industry 5.0: Human–computer interaction as a tech bridge from Industry 4.0 to Industry 5.0. In *Proceedings of the 9th International Conference on Web Research (ICWR)* (pp. 232–236). https://doi.org/10.1109/ICWR57742.2023.10139166

[4] Khan, L. U., *et al*. (2020). Resource optimized federated learning-enabled cognitive Internet of Things for smart industries. *IEEE Access, 8*, 168854–168864. https://doi.org/10.1109/ACCESS.2020.3023940

[5] Bolbotinović, Ž., Milić, S. D., Janda, Ž., & Vukmirović, D. (2025). AI-powered digital twin in the industrial IoT. *International Journal of Electrical Power & Energy Systems, 167*, 110656. https://doi.org/10.1016/j.ijepes.2025.110656

[6] Reyes-Acosta, R., *et al*. (2024). Analysis of machine learning-based approaches for securing the Internet of Things in the smart industry: A multivocal state of knowledge review. *International Journal of Information Security, 24*(1). https://doi.org/10.1007/s10207-024-00935-8

[7] Abdulrazzq, R. A., Sajid, N. M., & Hasan, M. S. (2024). Artificial intelligence-driven predictive maintenance in IoT systems. *South Florida Journal of Development, 5*(12). https://doi.org/10.46932/sfjdv5n12-030

[8] Romero, C. N., & Recto, K. H. A. (2025). IoT-driven hybrid microgrid simulation for energy-efficient smart industries. In *Proceedings of the IEEE International Conference on Industry 4.0, AI and Communications Technology (IAICT)* (pp. 628–632). https://doi.org/10.1109/IAICT65714.2025.11100678

[9] Rane, N., Choudhary, S., & Rane, J. (2023). AI and IoT-based sensors for monitoring and controlling in architecture, engineering, and construction. *SSRN Scholarly Paper* 4642197. https://doi.org/10.2139/ssrn.4642197

[10] Ghatge, S. K., & Parasar, A. (2023). Application of AI, IoT, and big data in healthcare, finance, and transportation. *SSRN Scholarly Paper* 4691289.

[11] Thotho, D., & Macheso, P. S. (2024). Comprehensive survey on applications of IoT, machine learning and AI in precision agriculture. *Tanzania Journal of Engineering and Technology, 42*(4), 30–45.

[12] Ayall, T. A., *et al*. (2025). Enhancing strawberry yield forecasting with backcasted IoT sensor data and machine learning. *arXiv*. https://doi.org/10.48550/arXiv.2504.18451

[13] Feng, H., Chen, D., & Lv, H. (2021). Sensible and secure IoT communication for digital twins, cyber twins, web twins. *Internet of Things and Cyber-Physical Systems, 1*, 34–44. https://doi.org/10.1016/j.iotcps.2021.12.003

[14] Al Rawajbeh, M., *et al*. (2025). Trustworthy adaptive AI for real-time intrusion detection in industrial IoT security. *IoT, 6*(3), 53. https://doi.org/10.3390/iot6030053

[15] Imran, G., *et al*. (2021). A topical review on machine learning, SDN, and IoT applications: Research limitations and challenges. *Electronics, 10*(8), 880. https://doi.org/10.3390/electronics10080880

[16] Rajavel, R., *et al*. (2022). IoT-based smart healthcare video surveillance system using edge computing. *Journal of Ambient Intelligence and Humanized Computing, 13*(6), 3195–3207. https://doi.org/10.1007/s12652-021-03157-1

[17] Demirbaga, U. (2025). EcoCloud: Green computing through energy and carbon efficient task scheduling in industrial IoT-enabled cloud environments. *IEEE Internet of Things Journal, 12*(17), 34644–34652. https://doi.org/10.1109/JIOT.2025.3537111

[18] Alsuwaelim, H. K. (2024). Exploring emerging cybersecurity risks from AI-based IoT connections. *Journal of Theoretical and Applied Information Technology, 102*(13).

[19] Popov, V. V., *et al*. (2022). Industry 4.0 and digitalisation in healthcare. *Materials, 15*(6), 2140. https://doi.org/10.3390/ma15062140

[20] Paul, S., *et al*. (2021). Industry 4.0 applications for medical/healthcare services. *Journal of Sensor and Actuator Networks, 10*(3), 43. https://doi.org/10.3390/jsan10030043

[21] Chen, J., *et al*. (2024). Generative-AI-driven human digital twin in IoT healthcare: A comprehensive survey. *IEEE Internet of Things Journal, 11*(21), 34749–34773. https://doi.org/10.1109/JIOT.2024.3421918

[22] Mwanza, J., Telukdarie, A., & Igusa, T. (2023). Impact of Industry 4.0 on healthcare systems of low- and middle-income countries. *Health and Technology, 13*(1), 35–52. https://doi.org/10.1007/s12553-022-00714-2

[23] Singh, S. P., *et al*. (2025). Federated learning-based multi-objective optimization for IoT-enabled distributed environmental monitoring. *IEEE Transactions on Consumer Electronics*. https://doi.org/10.1109/TCE.2025.3594404

[24] Mishra, A. (2025). AI-powered cybersecurity framework for secure data transmission in IoT networks. *International Journal of Advances in Engineering and Management, 7*(3), 5–13.

[25] Miller, T., *et al*. (2025). The IoT and AI in agriculture: The time is now. *Sensors, 25*(12), 3583. https://doi.org/10.3390/s25123583

[26] Adli, H. K., *et al*. (2023). Recent advancements and challenges of AIoT application in smart agriculture. *Sensors, 23*(7), 3752. https://doi.org/10.3390/s23073752

[27] Ibrahim, A. S., *et al*. (2025). AI-IoT based smart agriculture pivot for plant diseases detection. *Scientific Reports, 15*(1), 16576. https://doi.org/10.1038/s41598-025-98454-6

[28] Sasikumar, A., *et al*. (2022). Sustainable smart industry: A secure and energy efficient consensus mechanism for AI-enabled IIoT. *Computational Intelligence and Neuroscience*. https://doi.org/10.1155/2022/1419360

[29] Sujatha, M., *et al*. (2022). IoT and machine learning-based smart automation system for Industry 4.0. *Journal of Nanomaterials*. https://doi.org/10.1155/2022/6807585

[30] Islam, S. O. B., & Lughmani, W. A. (2023). A connective framework for safe human–robot collaboration in cyber-physical production systems. *Arabian Journal for Science and Engineering, 48*(9), 11621–11644. https://doi.org/10.1007/s13369-022-07490-

.