Proceedings of the 3rd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/118/2025.20805

# *AIoT: The Integrating of Artificial Intelligence and the Internet of Things*

**Weijie Liu**[1,a,*]

[1]*Guangdong University of Technology, Guangzhou, China*
*a. 3123009086@mail2.gdut.edu.cn*
**corresponding author*

***Abstract:*** At present, artificial intelligence has emerged as a significant field all over the world, offering diverse enhancements across many industries when combined with it. This study primarily examines the combination of the Internet of Things and artificial intelligence, highlighting practical applications and areas requiring enhancement. Mainly from a literature review utilising the three keywords: artificial intelligence, the Internet of Things, and application for search and screening, it was discovered that there are several issues in the application of this field. There are issues with delayed data transmission, compatibility, and anomaly detection in the field of autonomous driving. In the field of wearable devices, there are data security issues. In the field of industrial Internet of Things, there are problems such as low transmission efficiency, high latency, and inability to effectively resist external network attacks. In addition, there are also trust issues in the field of artificial intelligence where decisions and predictions cannot be understood by people. In besides this, this study provides several of recommendations for improvements in further research.

***Keywords:*** Artificial Intelligence, Internet of Things, Application

## 1. Introduction

With the continuous development of science and technology, the Internet of Things industry is also constantly improving. The rise of artificial intelligence has brought a higher ceiling and more room for improvement to this industry. Therefore, the combination of artificial intelligence and the Internet of Things is also the general trend of the future.

In the past five years, IoT technologies have also been well developed and advanced, such as: sensors, wireless communication, cloud computing, big data, etc. In addition, the Internet of Things is widely used in this field, such as: smart transportation, smart home, and the industrial Internet of Things. Most of them already have a good development and market. However, they still have some limitations. For example: data security, data integrity and accuracy, the high cost of IoT devices, and the interoperability between devices. The addition of artificial intelligence can effectively solve some problems and give birth to many new products, including driverless cars, smart wearable devices, the industrial Internet, smart home, etc., but there are still various problems in these fields, first of all, we have no recognition of the credit problems of these applications. The safety, accuracy and ability of the car to deal with special situations. Secondly, how can we make some elderly or disabled people better use these emerging products, which requires us to consider simplifying the operation interface or use steps. Finally, it is whether data security can be guaranteed.

DOI: 10.54254/2755-2721/118/2025.20805

This article mainly describes how artificial intelligence solves the problems of the Internet of Things. It includes a specific explanation of the nature of AI and how these properties can solve the problems of the Internet of Things. Additionally, it outlines a new product that combines IoT and artificial intelligence. Specifically, it includes the introduction and development space of each product.

## 2. The auxiliary role of artificial intelligence

### 2.1. The transmission capability of artificial intelligence

There is a compatibility problem between the Internet of Things, and we can optimize data processing through artificial intelligence, so that data can be transmitted to each other efficiently and accurately. Besides, Artificial intelligence enhances wireless transmission to improve reliability and security in heterogeneous and even hostile environments [1]. Artificial intelligence can reduce external interference and protect the data transmission process, thereby enhancing the security of data.

Artificial intelligence technology plays an important role in intelligent transmission networks. Through machine learning and deep learning algorithms, the network can autonomously identify abnormal traffic, automatically adjust configurations, and optimize transmission paths, thereby greatly improving the response speed and efficiency of the network. In addition, the application of Internet of Things (IoT) technology has further expanded the range of applications by enabling intelligent transport networks to connect more devices and sensors.

### 2.2. Explainable artificial intelligence(XAI)

Current methodologies in Artificial Intelligence (AI) have shown high capabilities in prediction and processing speed, however, the models lack transparency and explanations. XAI can effectively solve these problems [2]. XAI-Interpretive Artificial Intelligence refers to an artificial intelligence model that can explain its decision-making process, enabling humans to understand its inner workings and the basis for its decision-making. XAI model interpretation methods are different, and these methods can provide explanations and make the prediction process more transparent, so there is no one standard answer to the interpretation of the model. are all ways to contribute to human understanding [3].

XAI's goal is to improve the interpretability and transparency of models, thereby increasing users' trust and understanding of models, and helping to address issues such as AI ethics and bias.

### 2.3. Cloud-based intelligence in artificial intelligence

The IoT device uploads the collected data to the cloud platform, and the cloud AI performs deep learning and large-scale data analysis through powerful cloud computing capabilities, and then sends the analysis results back to the device for intelligent control. Cloud intelligence has been widely used in various practical applications, such as intelligent transportation, intelligent industry, etc [4][5].

## 3. Applications of AIoT

### 3.1. Self-driving car

In this section, it mainly describes the development of driverless cars and some improvement suggestions, the emergence of driverless cars, has brought us a lot of convenience, driverless cars can help station people and the elderly to travel. To a certain extent, it can also alleviate fatigue driving and reduce the occurrence of drunk driving. Autonomous vehicles can share data through 5G or 6G signals [1]. This data includes sharing traffic conditions, sharing where accidents occurred, etc. By uploading this data to the cloud, AI can reasonably plan the travel route of each car through this data,

DOI: 10.54254/2755-2721/118/2025.20805

and can also reasonably explain the reason for this route to people through XAI, thereby increasing people's understanding and trust in the car's planning route [6]. And this rational planning also reduces traffic congestion to a certain extent. However, this planning distribution can also lead to an increase in the accident rate, because each car simply executes the order, and if there is an emergency, the accident may occur because the order is not changed in time. There is a certain delay in the transmission of information to and from the vehicle, so if the vehicle is unable to obtain the information in time, it may also lead to accidents. Therefore, we need to improve the efficiency and accuracy of data transmission. Driverless cars also need to have vehicle anomaly detection, which includes the outside world and itself, and anomaly detection can be carried out through intelligent sensors [5] to detect and make reasonable decisions and share information in a timely manner. In the future, driverless cars will not be made by one company, so when it comes to data sharing, we need to consider compatibility issues and artificial intelligence to help us solve this problem. In addition, pedestrian detection is also an important aspect that we cannot ignore, and the main focus here is on the detection of some vulnerable groups such as people with disabilities. They can signal the car by wearing a WPD (Wearable Personal Device), and the on-board unit in the car, the OBV, can receive the signal in real time and notify the car that a person with a disability is passing by [7]. A series of measures have been taken to improve the field of driverless cars.

### 3.2. Wearable Internet of Things(XAIoT)

At present, many types of professional equipment have been developed, including smart helmets, smart thermometers, smart wristbands, smart watches and other smart products [8]. A large part of these wearable devices are mainly used in medical applications, where these devices can monitor the patient's physical condition in real time and send it to the appropriate doctor and artificial intelligence in a timely manner. Artificial intelligence can make reasonable predictions through big data, and use XAI to tell people the cause of the disease in a timely manner, and some precautions. There have been inventions to implement XAIoT with the Empatica E4 wristband device and the corresponding program [2]. Doctors can access the patient's data directly for telemedicine, without the patient having to visit the hospital in person, so as to achieve the best possible patient treatment. These systems are not only physical (blood pressure, temperature, heart rate, etc.) but also psychological (emotion, etc.). In addition, due to the variety of wearable devices, there is a corresponding demand for the flexibility of electronic components. And flexible electronic files can be well combined with smart socks, smart clothes and other related smart products. These wearables can not only be used for detection, but also as a technological fad [9]. However, there are still some security issues in wearable devices, the most prominent security risk is whether the data privacy of patients can be reasonably protected. There are also workarounds, such as defending against external attacks through federated learning [10], thus protecting the security of data.

### 3.3. Industrial internet of things

In recent years, with the emergence of relevant policies, the development of the industrial Internet of Things has entered a period of rapid growth, and the application fields of the industrial Internet of Things are also very wide, including intelligent manufacturing, smart cities and intelligent transportation. After the emergence of artificial intelligence, the industrial Internet has obtained technological integration and innovation, which is also known by many as the industry entering the 4.0 era [11]. Many problems of the industrial Internet have also been solved with the assistance of artificial intelligence. and the problem is mainly concentrated in three properties [12]. First of all, it must be operable. As initialization evolves, people in the city must receive a higher level of training to complete assigned tasks. They can be guided by artificial intelligence to better assist them in

DOI: 10.54254/2755-2721/118/2025.20805

completing assigned tasks. Artificial intelligence can also simplify operations to a certain extent. The second is how portability can effectively reduce latency, which is something we need to consider. At present, there are related methods that can effectively reduce latency, such as a deterministic scheduling method based on non-conflict theory to achieve ultra-low latency of time-sensitive streams, and a dynamic queue scheduling method to improve broadband utilization [13]. Finally, there is the issue of intractability. Our artificial intelligence can see the internal identification and transformation, so that the data can be accurately transferred between various systems. However, the security risks of the industrial Internet also require our attention. Since AI is automated, it can continuously track security breach specifications, which is also something we can't do humans. Of course, there are also proposals to strengthen intrusion detection and design a platform that can identify different attacks [14], which can complement artificial intelligence.

## 4. Challenges

At present, there are still many deficiencies and challenges in this field, the first of which is the safety and uncertainty of products, which leads to people's problems [1]. Nowadays, some cars have the function of unmanned driving, but the number of people who try it is still relatively small. The second is to make the operating system more relevant to ordinary people, so that decisions can be made more easily understood by people [15]. For example, it is possible to interact with people in different regions using different dialects, etc. On top of that, there's the security of your data. This data includes personal information data, industrial data, etc [5]. Finally, how to effectively reduce latency and make data transmission more efficient.

## 5. Future Directions

### 5.1. Simplify the operating system

Operating systems need to be simpler, more efficient, and more responsive to vulnerable groups such as the disabled or the elderly. At present, these emerging products of the Internet of Things mainly serve young and middle-aged people. For example, in smart homes, some young people need to learn how to use them. Older people have weaker learning and acceptance abilities, so they need simpler operating systems. Smart devices can introduce some elderly modes, allowing them to also enjoy convenience. The needs of people with disabilities are also different from those of ordinary people, so intelligent features such as sign language recognition can be added, or the operating system can be simplified so that they can use these devices.

### 5.2. Low latency transmission

With the rapid increase in real-time applications, the demand for latency is also increasing, effectively reducing latency, thereby improving the efficiency of data transmission and improving the feedback speed of multiplicity. In the field of industrial Internet of Things, effective coordination between machines is achieved through data transmission, and high latency may cause problems in the coordination between machines. The machine that originally needed to perform the next level task is still executing the previous level task, and errors in intermediate stages can also affect subsequent stages. In case of emergencies, the machine may be damaged due to delay issues. For example, if a machine recognizes an incorrect material and cannot respond in a timely manner, it may cause damage to the material or machine.

DOI: 10.54254/2755-2721/118/2025.20805

### 5.3. Measures to deal with hostile environments

We need to strengthen the safety of our products, the security, the basis on which all products are accepted and this security, both external and internal. External safety is the reliability of the product, whether the product has the possibility of harm to the human body. Internal security is data security, and ensuring that data will not be leaked also requires our attention.

## 6. Conclusion

This study mainly reviews the application of the combination of artificial intelligence and the Internet of Things and provides solutions to some existing problems. However, some of the research stops at theory and does not have practice, so the follow-up research mainly wants to study in practice.

## References


[1] *M. Karner, J. Hillebrand, M. Klocker and R. Sámano-Robles, "Going to the Edge - Bringing Internet of Things and Artificial Intelligence Together," 2021 24th Euromicro Conference on Digital System Design (DSD), Palermo, Italy, 2021, pp. 295-302, doi: 10.1109/DSD53832.2021.00052.*

[2] *R. Krzysiak, S. Nguyen and Y. Chen, "XAIoT - The Future of Wearable Internet of Things," 2022 18th IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications (MESA), Taipei, Taiwan, 2022, pp. 1-6, doi: 10.1109/MESA55290.2022.10004460.*

[3] *A. B. Arrieta, N. Díaz-Rodríguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, S. García, S. Gil-López, D. Molina, R. Benjamins et al., "Explainable artificial intelligence (xai): Concepts taxonomies opportunities and challenges toward responsible ai", Information fusion, vol. 58, pp. 82-115, 2020.*

[4] *Radu, F.; Cotfas, P.A.; Alexandru, M.; Bălan, T.C.; Popescu, V.; Cotfas, D.T. Signals Intelligence System with Software-Defined Radio. Appl. Sci. 2023, 13, 5199. https://doi.org/10.3390/app13085199*

[5] *César Bautista* and Gyula Mester Óbuda'INTERNET OF THINGS IN SELF-DRIVING CARS' ENVIRONMENT University, Doctoral School of Safety and Security Sciences Budapest, Hungary DOI: 10.7906/indecs.21.2.8 Regular article ABSTRACT Received: 17 December 2022. Accepted: 28 February 2023.*

[6] *Nwakanma, C.I.; Ahakonye, L.A.C.; Njoku, J.N.; Odirichukwu, J.C.; Okolie, S.A.; Uzondu, C.; Ndubuisi Nweke, C.C.; Kim, D.-S. Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review. Appl. Sci. 2023, 13, 1252. https://doi.org/10.3390/app13031252*

[7] *Guerrero-Ibañez, A.; Amezcua-Valdovinos, I.; Contreras-Castillo, J. Integration of Wearables and Wireless Technologies to Improve the Interaction between Disabled Vulnerable Road Users and Self-Driving Cars. Electronics 2023, 12, 3587. https://doi.org/10.3390/electronics12173587*

[8] *Subhan, F.; Mirza, A.; Su'ud, M.B.M.; Alam, M.M.; Nisar, S.; Habib, U.; Iqbal, M.Z. AI-Enabled Wearable Medical Internet of Things in Healthcare System: A Survey. Appl. Sci. 2023, 13, 1394. https://doi.org/10.3390/app13031394*

[9] *Royo, I.; Fernández-García, R.; Gil, I. Microwave Resonators for Wearable Sensors Design: A Systematic Review. Sensors 2023, 23, 9103. https://doi.org/10.3390/s23229103*

[10] *M. Ali, F. Naeem, M. Tariq and G. Kaddoum, "Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 778-789, Feb. 2023, doi: 10.1109/JBHI.2022.3181823.*

[11] *Barari, A., de Sales Guerra Tsuzuki, M., Cohen, Y. et al. Editorial: intelligent manufacturing systems towards industry 4.0 era. J Intell Manuf 32, 1793–1796 (2021).*

[12] *Valle PTonon VGarcés LRezende SNakagawa E(2025)TASIS: A typology of architectural strategies for interoperability in software-intensive systems Computer Standards & Interfaces 10.1016/j.csi.2024.10387491(103874)Online publication date: Jan-2025https://doi.org/10.1016/j.csi.2024.103874*

[13] *Y. Lu et al., "An Intelligent Deterministic Scheduling Method for Ultralow Latency Communication in Edge Enabled Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1756-1767, Feb. 2023, doi: 10.1109/TII.2022.3186891.*

[14] *Y. Zhang, C. Yang, K. Huang and Y. Li, "Intrusion Detection of Industrial Internet-of-Things Based on Reconstructed Graph Neural Networks," in IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, pp. 2894-2905, 1 Sept.-Oct. 2023, doi: 10.1109/TNSE.2022.3184975.*

[15] *A. B. Arrieta, N. Díaz-Rodríguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, S. García, S. Gil-López, D. Molina, R. Benjamins et al., "Explainable artificial intelligence (xai): Concepts taxonomies opportunities and challenges toward responsible ai", Information fusion, vol. 58, pp. 82-115, 2020.*