A Survey: The Uses of Artificial Intelligence of Things (AIOT): Possible Advantages and New Trends

Mohammed H. Alabiech
General Company of Electrical Energy Production – Southern Region, Ministry of Electricity, Basra, Iraq

Sanaa Ali Jabber
Al-muthanna University, Al-muthanna, Iraq

Wala'a N. Jasim
Department of Pharmacognosy, College of Pharmacy, University of Basra, Basra, Iraq

ABSTRACT

The Internet of Things (IoT) and Artificial Intelligence (AI) are each considered powerful and promising technologies in the IT sector. When combined, they form a more advanced concept known as the Artificial Intelligence of Things (AIoT). In this survey, IoT devices act as a digital nervous system, while AI serves as the system's mastermind. This article provides a brief overview of this hybrid technology and explores some of its practical applications in the real world, in addition to the role of AI algorithms in addressing potential security threats.

General Terms

Internet of Things, Artificial Intelligence, Machine Learning, Deep Learning

Keywords

Internet of Things (IoT), Artificial Intelligence (AI), AIoT Deep Learning, Machine Learning

1. INTRODUCTION

Due to its autonomous nature and ability to make independent decisions, AI is establishing its own distinct role. The IoT comprises a growing number of connected devices, ranging from smart homes and highways to a fully interconnected world. Intelligent IoT is poised to profoundly transform not only daily life but society as a whole [1].

Both IoT and AI have been the subject of ongoing research. Many AI problem-solving algorithms have been proposed. Most of these are still in the early stages of development but are expected to evolve over time. These algorithms are capable of processing massive volumes of data and making intelligent decisions independently [2]. Meanwhile, the IoT has already made significant progress, and it seems to be only a matter of time before are fully surrounded by IoT devices. AIoT represents a hybrid of IoT and AI technologies [3].

AIoT will extend current standards of IoT to create autonomous future communication architectures that will facilitate the intelligent exchange of data between millions of devices [4]. Using intelligence in cutting-edge network paradigms such as Network Function Virtualization (NFV), Software-Defined Networks (SDN), and network slicing architectures will improve network resource consumption even further [5]. Agriculture, health care, security, smart homes, and autonomous vehicles are just a few of the AIoT applications that will soon become essential [6].

This work offers an extensive overview of internet o things (AIOT) applied with ARTIFICIAL INTELLIGENCE techniques. The presented work is structured as follows: Section 2 reviews state-of-the-art research on the application of artificial intelligence for IoT .Section 3 details the methodology used to identify and select the most relevant studies in the field, while Section 4overview about Where does AI unlock IoT, Section 5 explain The most important advantages of the Internet of Things supported by artificial intelligence. On the other hand, Section 6 gives realistic models of artificial intelligence . Section 7 discusses the benefits of AI-based Smart security for the Internet of things, while Section 8 highlights security attacks on IOTs. On the other hand, Section 9 explore outlines presented work applications of deep learning (DL) and machine learning (ML) in the IOT security . Finally, Section 10 presents the conclusions of the study and future works.

2. STUDY SELECTION

Along with manual screening of relevant sources, a thorough literature search utilizing many academic databases was undertaken. Such databases included Google Scholar, ResearchGate, Web of Science, Scopus, and IEEE Xplore. Initially, we found 4000 studies on artificial intelligence and internet of things. To guarantee relevance, these studies were filtered depending on their emphasis on efficient artificial intelligence for internet of things techniques. This yielded 40 research papers that were then exposed to in-depth analysis. The selected papers were examined more closely to create a suitable internet of things system by using artificial intelligence that would help to clearly define their contributions and methodological differences. Based on the utilized models, Fig.1 presents the main categories that were obtained.

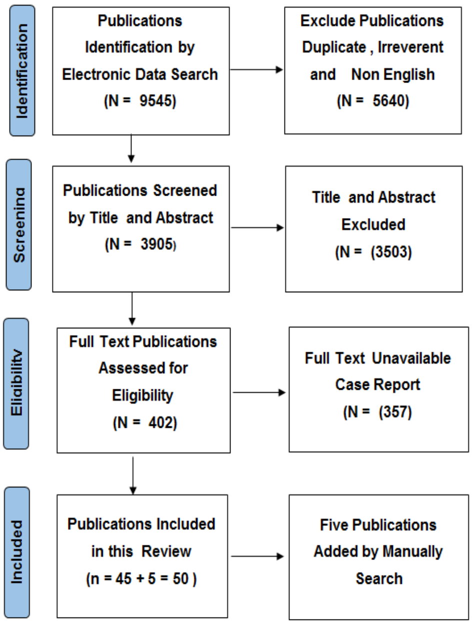

Identification
Publications Identification by Electronic Data Search (N = 9545)
Exclude Publications Duplicate , Irreverent and Non English (N = 5640)
Screening
Publications Screened by Title and Abstract (N = 3905)
Title and Abstract Excluded (N = (3503)
Eligibility
Full Text Publications Assessed for Eligibility (N = 402)
Full Text Unavailable Case Report (N = (357)
Included
Publications Included in this Review (n = 45 + 5 = 50)
Five Publications Added by Manually Search

Fig. 1. PRISMA flowchart of included researches

3. RELATED WORKS

Referred to as the Artificial Intelligence of Things (AIoT), has gained significant attention in recent years. Several studies have explored its applications across diverse domains. For instance, AIoT has been applied in smart healthcare systems to enable real-time patient monitoring and predictive diagnostics. In industrial environments, AIoT facilitates predictive maintenance, process optimization, and energy management. Moreover, smart cities benefit from AIoT through intelligent traffic management, environmental monitoring, and automated public services. Previous works also highlight the crucial role of AI in enhancing data analysis, decision-making capabilities, and security measures for IoT ecosystems, addressing vulnerabilities inherent in low-cost and resource-constrained devices. Despite these advancements, challenges such as scalability, interoperability, and robust security mechanisms remain open areas for research, motivating ongoing studies.

"The related works on this topic are summarized in Table 1."

4. WHERE DOES AI UNLOCK IOT?

IoT is primarily about sensors embedded in machines, which provide data streams through internet access. Communicate, create, analyze, aggregate, and act represent the five main stages that any IoT-related service has to follow. Without a doubt, the value of the "Act" stage is determined by the final analysis. This is why the true value of IoT is realized during the analysis phase. This is where AI plays a crucial role [14]. While IoT presents data, AI has the capability to unlock insights, provide context, and enable creative, smart actions. Businesses can make informed decisions based on data collected by sensors, which can be analyzed using AI. AIoT enables the development of agile, next-generation solutions [15].

- Obtain, analyze and manage meaningful insights from data.
- Ensure precise and rapid analysis.
- Balance personalization with data privacy and confidentiality.
- Balance requirements for centralized and localized intelligence.
- Ensuring security against cyber-attacks.

5. ADVANTAGES of AI ENABLED IOT

Artificial intelligence in IoT provides many different advantages for consumers as well as businesses, including personalized experiences, proactive interventions, and intelligent automation. Below are a few of the most common commercial advantages of merging these two disruptive technologies:

5.1 Predictive maintenance

Equipment breakdown might lead to costly unplanned downtime in a variety of industries, such as offshore oil and gas and industrial production. Predictive maintenance using AI-enabled IoT allows for anticipating equipment failure and arranging routine maintenance procedures ahead of time. This is why one can prevent the negative consequences of downtime [16], [17]. With IoT and AI, for instance, Deloitte finds the following outcomes:

20% - 50% decrease in the time invested for maintenance planning.

10% - 20% increase in the uptime and the availability of the equipment.

5% - 10% decrease in the costs of maintenance.

A real-world case study from the Siemens Amberg smart factory in Germany illustrates the practical effectiveness of AIoT-based predictive maintenance. By using over 1,000 IoT sensors and AI algorithms such as Random Forest and RNNs, Siemens achieved a 30% reduction in unexpected equipment failures, over 10% in maintenance cost savings, and an 8% increase in overall equipment efficiency [18].

5.2 Triggering New and Enhanced Products & Services

Natural Language Processing (NLP) is enhancing individuals' capability to communicate with machines. Without a doubt, combining IoT with AI may help businesses build new products or improve existing ones by allowing them to analyze and process data more quickly [19]. For example, Rolls-Royce intends to utilize AI to develop IoT-enabled aircraft engine maintenance facilities. This approach will aid in detecting trends and discovering operational insights [20], [21].

5.3 Better Risk Management

The combination of IoT and AI allows businesses to better predict and analyze many different kinds of danger, as well as automate responses. This is why they are better equipped to deal with financial losses, cyber threats, and personnel safety [15], [16]. Fujitsu, for instance, utilizes AI to analyze data from connected wearable devices to ensure worker safety [21].

Table 1: Summary of Some Related Works

Ref.	Year	summary	Methodology	Limitation
[7]	2020	The paper analyzes the applications and real-time examples of the artificial intelligence of things (AIoT).	The methodology involves analysis of AIoT and its applications, focusing on descriptive or exploratory approaches.	-
[8]	2022	The integration of AI and IoT, known as AIoT, can create public value by improving public service delivery.	- Descriptive-explanatory study - Qualitative approach - Thorough examination of drivers and barriers - Development of a conceptual framework	- Limited understanding of how AIoT can improve public service delivery - Need for further research to create a modular framework for AIoT integration - Gap in understanding AIoT for policy formulation

[9]	2022	The paper discusses the role of artificial intelligence in making IoT a transformative technology.	The methodology involves a comprehensive review of the Internet of Things (IoT) technology, focusing on its current state, enabling technologies, applications, and grand challenges. It includes an analysis of the role of artificial intelligence in IoT and an examination of current issues and potential barriers to adoption.	- Privacy and security concerns - Data heterogeneity and device interoperability issues - Unrestricted access control - Small footprint and resource constraints of IoT sensors - Lack of a unified ecosystem for IoT devices - Security concerns with cloud-hosted middleware layers - Exposure to internet vulnerabilities - Difficulty in determining responsibility within distributed systems - Challenges in reviewing privacy policies due to device size limitations - High cost of implementing predictive maintenance (PdM)
[11]	2023	AIoT offers transformative potential for agriculture by optimizing resource utilization, improving production management, and reducing labor dependency, but also faces challenges such as data quality, connectivity, cost, privacy, and user adoption.	-	- Data quality issues - Connectivity problems - High costs - Privacy concerns - User adoption difficulties - Need for advanced AI algorithms - Need for edge computing - Need for interoperability standards - Need for investigation into AIoT's role in climate resilience and resource management - Need for research on AIoT adoption and usability - Need for research on social and ethical implications - Need for research on AIoT-based supply chain integration
[12]	2024	AIoT combines AI and IoT to enable more efficient and improved IoT operations and services with enhanced data management and analysis capabilities.	-	-
[13]	2024	The paper explores the advantages and ethical considerations of using Industrial IoT and AI (AIoT) solutions in smart manufacturing, robotics, and autonomous vehicles.	- Integrative study of leading scientific publications on IIoT and AIoT - Use of PRIZMA flow chart for document filtering - Content analysis in thematic groups	- The inability to fully cover the AIoT topic in one article, necessitating content analysis in several thematic groups.
[14]	2024	The paper discusses how the integration of AI and IoT, known as AIoT, can enable smart, eco-friendly manufacturing systems with improved efficiency, automation, and security.	The study involves a comprehensive review of industry technologies for domain-centric, AIoT-based sustainable manufacturing, examining key developments and opportunities in state-of-the-art AIoT-based techniques.	

5.4 Boosting Operational Efficiency

AI in IoT analyzes continuous data streams and discovers patterns that cannot be detected by simple gauges. In addition, machine learning combined with AI can forecast operating conditions and identify parameters that should be adjusted to achieve optimal results. As a result, intelligent IoT can reveal procedures that are redundant and time-consuming, as well as tasks that can be fine-tuned to improve efficiency [25], [26]. Google, for instance, utilizes AI to lower the expenses of its data center cooling through IoT [27].

6. REALISTIC MODELS OF AIOT

The combination of IoT and effective frameworks makes AIoT an important and game-changing tool for a variety of purposes [27], here are a few examples:

6.1 Drone Traffic Monitoring

There are various realistic AIoT applications in a smart city, including traffic monitoring via drones. Jamming might be reduced if traffic could be inspected in real-time and changes to the traffic flow are made.

In cases when drones are dispatched to oversee a large area, they may broadcast traffic data, which AI can then analyze and produce conclusions on how to optimally alleviate the traffic congestion through adjusting the frequency and timing of the traffic lights, without the need for any human intervention.

The ET City Brain, a result of Alibaba Cloud, streamlines the utilization of city assets through AIoT. This framework can recognize accidents, illegal parking, as well as adjust traffic lights to assist ambulances in reaching patients who require support more quickly [28], [29].

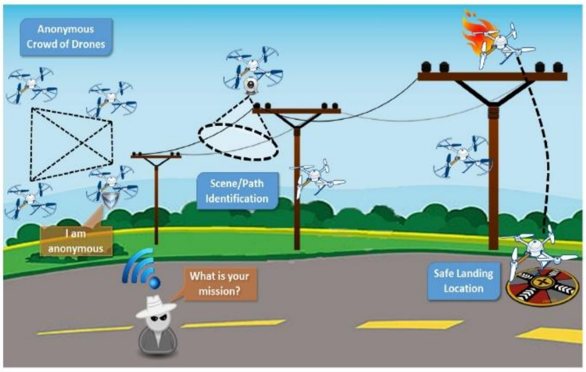


Fig. 2: Traffic Monitoring Using Drone

6.2 Robots in Manufacturing

Manufacturing can be defined as an industry that has already embraced novel technologies like AI, IoT, deep learning, robotics, facial recognition, and others. With the help of embedded sensors facilitating data transmission, factory robots are becoming smarter. In addition, robots can learn from new data because they are equipped with AI systems. This approach saves both money and time while improving the production process over time [30], 31].

The best example of AI and IoT working together is Tesla's self-driving cars. These vehicles use AI to predict pedestrian and vehicle behavior in various situations. For instance, they can identify road conditions, weather, and optimal speed, and they become smarter with every trip. Tesla's autopilot systems use sonar, radar, GPS, and cameras to collect information about driving conditions, which is then processed by an AI system to make decisions based on the data collected by the IoT devices [28], [32].

6.3 Retail Analytics

Several data points from cameras and sensors are utilized in retail analytics to track customer movements and forecast when they will arrive at the checkout line. As a result, the system can recommend dynamic staffing levels to reduce checkout times and boost cashier productivity [33], [34].

6.4 Digital Halthcare

Digital healthcare is one of the most prominent domains that can benefit from AI-enabled functionality, especially with the current boom in AI, particularly deep learning methods [24].

6.5 Smart Metering and Smart Grids

Smart metering encompasses a wide range of monitoring, measurement, and management applications. Smart grids, where electricity usage is monitored and recorded, represent the most typical application of smart metering. In addition, smart metering can also be used to combat electricity theft [35]. It can further be applied to monitor the levels of oil, water, and gas in storage tanks and cisterns [36], as shown in the Figure 3.

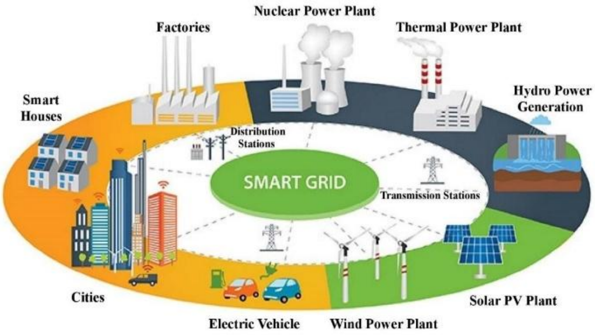


Fig. 3: Diagram of a Smart Grid Showing a Few

7. INTELLIGENT SECURITY For THE IOT

IoT device security has become one of the most pressing issues of this century. On one hand, IoT brings everything closer together and has connected the entire planet. Figure 4 represents the estimated number of IoT device users by the year 2024. Figure 5 depicts a graphical representation of the total connected IoT devices and the global IoT market up until now, along with future predictions. On the other hand, IoT has opened up many opportunities to be exploited by various types of attacks. Although the term IoT has been shortened in this context, it encompasses the entire world as well as its smart technologies and services, which can be imagined. The term IoT was first used in 1999 by Kevin Ashton in his research. Since then, IoT has been used to establish a connection between the human and virtual worlds through a variety of smart devices and services, utilizing a range of communication protocols [37].

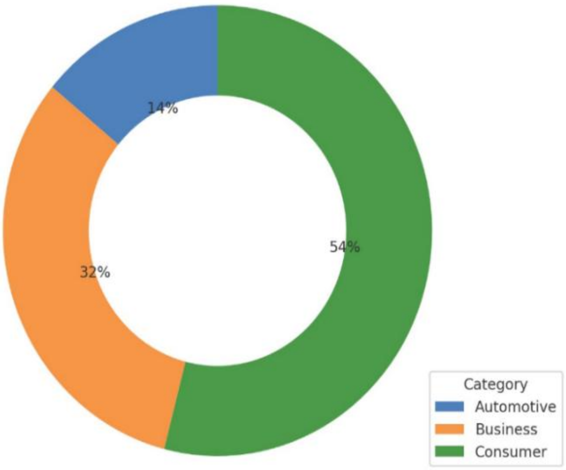


Fig. 4: Estimated users of the IoT devices by 2024.

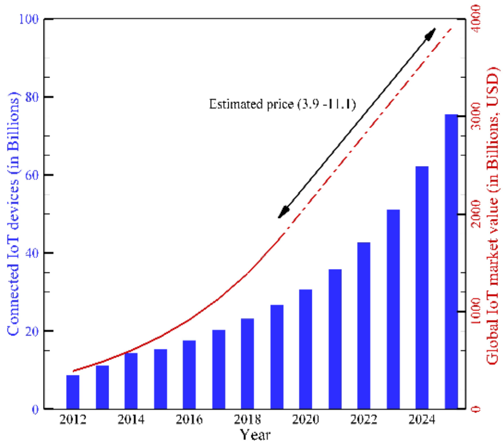


Fig. 5: Graphical presentation of the total connected IoT devices and the global IoT market up until the end of the year 2025

What has been merely an imagination a quarter of a century ago has now become an actual reality thanks to the IoT. It can be said that the modern world has been wrapped by the smart technology and IoT represents its heart. Nowadays, the people are not capable of thinking even a moment on their own without the use of the IoT devices as well as their services. A study has shown that about 75 billion things will be connected to the internet by the end of the year 2025 and this number will be exponentially increased with time. Estimated percentage of the users of the IoT devices in the year of 2024 has been depicted in Figure 4. It has been estimated as well that the IoT will capture about 3.90−11.10 trillion $ economical markets by the year of 2025. The number of connected IoT devices and global IoT system markets up until the end of the year 2025 has been depicted in Figure 5. Which is why, the researches about the IoT as well as its security and development had gained a great deal of attentions throughout the past decades in electrical and computer since areas. The two sections below will include a discussion of the security challenges and layers of the IoT [37].

8. SECURITY ATTACKS ON IOTS

Figure 6 illustrates a common architecture of the IoT. Several researchers have pointed out the fact that IoT technology operates on three layers, which are: perception, network, and application layers. The perception layer includes a variety of data sensor types, such as barcodes, RFID, or any other sensor networks. The goal of this layer is to obtain information from the environment using sensors and then send that information to the network layer [38].

The goal of the network layer is to transmit data obtained from the perception layer to a specific information processing system via a mobile network, the internet, or any other reliable network type. The goal of the IoT in developing a smart environment has been carried out in the application layer [37]. IoT security has been considered one of the biggest challenges due to its heterogeneity, complexity, and numerous interconnected resources. The attacker is capable of performing an attack on the IoT system by tampering with or damaging one of the nodes (i.e., physical vulnerability), or from within the network by exploiting routing protocol faults or other network protocols, or using a malicious program to break the encryption strategy (i.e., encryption attacks). Based on these vulnerabilities, attacks can be classified into four categories, as shown in Figure 6, which depicts the IoT physical attack architecture, software attack, network attack, and encryption attack. For each category, one attack has been selected as the most dangerous among all the attacks in that category.

Among physical attacks, the malicious node injection attack is considered the most dangerous. This is because it not only disrupts services, but also modifies data. Among network attacks, the sinkhole attack is identified as the riskiest. It not only attracts all traffic toward a base station, but also allows the attacker to initiate other threats such as selective forwarding, packet dropping, or modification. Among software attacks, the worm attack is considered the most harmful. Worms are potentially one of the most dangerous and destructive forms of malware on the internet. A worm is defined as a self-replicating program that exploits security vulnerabilities in networking hardware or software to cause harm to the device. It can delete files from the system and steal information [40].

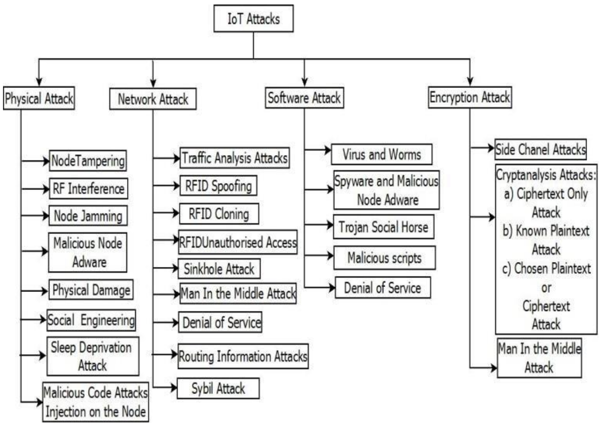


Fig. 6: Physical Attacks, Network Attacks, Software Attacks, and Encryption Attacks

9. Applications of Deep Learning (DL) and Machine Learning (ML) in the IOT Security

Learning algorithms are widely used in a broad range of real-world applications due to their remarkable ability to solve problems. These algorithms can build systems that automatically learn and improve over time through experience. Recently, they have been widely applied in practical domains. The development of current learning algorithms has been enhanced by the creation of new algorithms, the availability of big data, and the emergence of methods with lower computational costs. DL and ML have evolved significantly in recent years, progressing from mere laboratory curiosities to practical tools with substantial applications. Although deep learning is a branch of machine learning, this study distinguishes between the two: the term Machine Learning (ML) refers to traditional methods that require the manual design of features, while Deep Learning (DL) refers to modern approaches that use nonlinear processing layers to extract and transform analytical or discriminative features for pattern analysis [37],[40].

9.1 ML Methods For IoT Security

ML is an AI technique that trains machines using various approaches and enables devices to learn from experience rather than through explicit programming. ML does not require human assistance or complex mathematical formulas and can operate in dynamic networks. In recent years, ML approaches have significantly advanced in the field of IoT security. As a result, these approaches can be used to detect various IoT attacks at early stages by analyzing device behavior. Furthermore, appropriate solutions can be provided using different ML algorithms tailored for resource-constrained IoT devices [25].

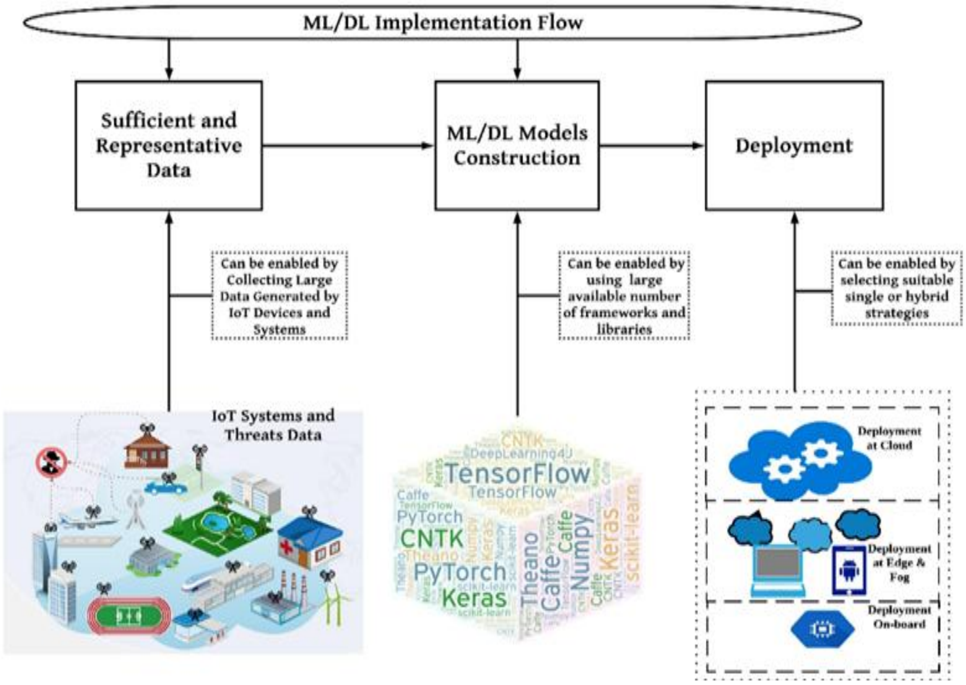
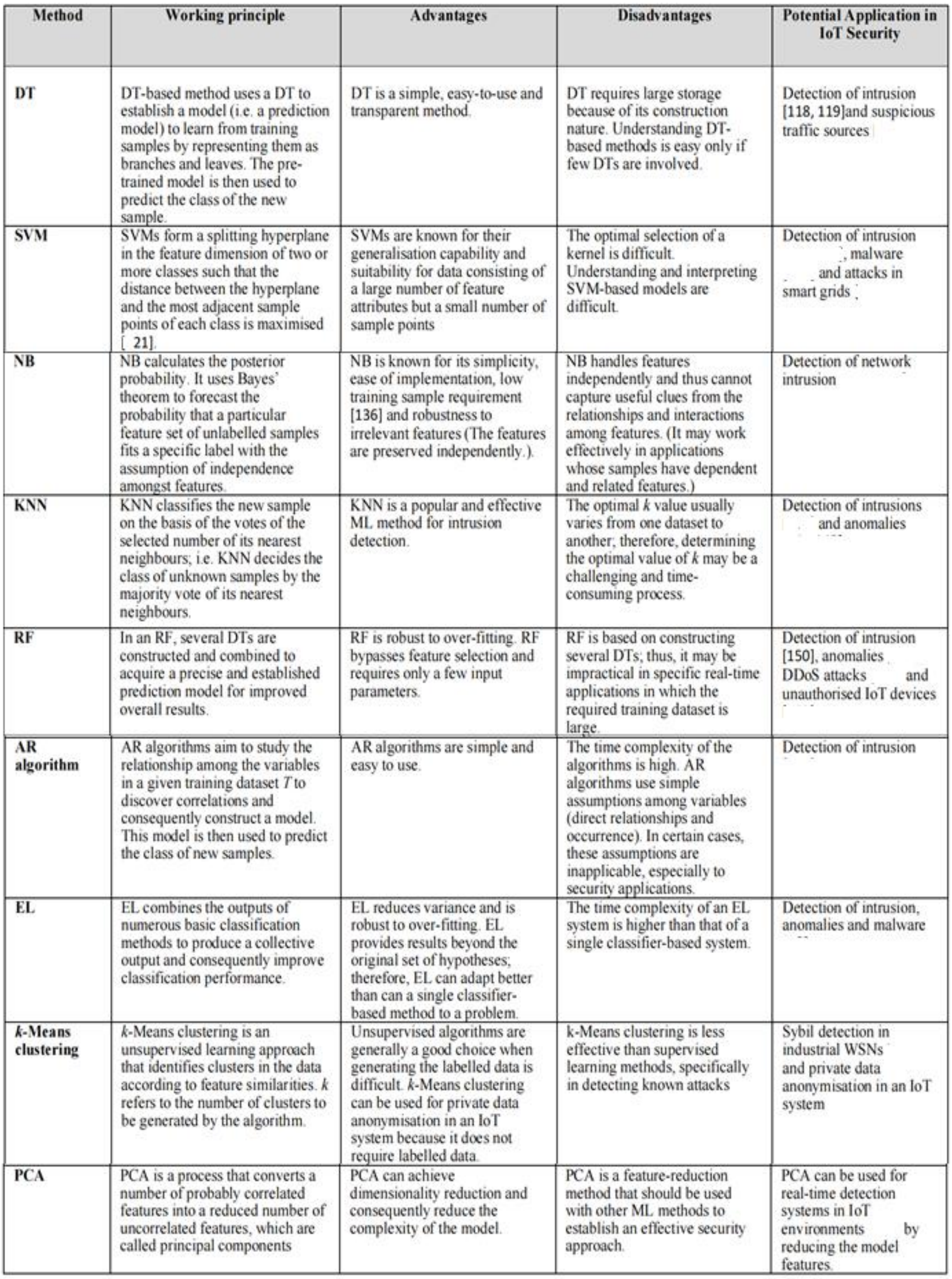

ML/DL Implementation Flow
Sufficient and Representative Data
ML/DL Models Construction
Deployment
Can be enabled by Collecting Large Data Generated by IoT Devices and Systems
Can be enabled by using large available number of frameworks and libraries
Can be enabled by selecting suitable single or hybrid strategies
IoT Systems and Threats Data
TensorFlow
CNTK
DeepLearning4J
PyTorch
Keras
Caffe
Theano
Numpy
scikit-learn
Deployment at Cloud
Deployment at Edge & Fog
Deployment On-board

Fig. 7: Technological Tools That Fundamentally Enable the Deployment of ML/DL for IoT Security

Table 1. Potential Machine Learning Methods for IoT System Security [40]



Method	Working principle	Advantages	Disadvantages	Potential Application in IoT Security
DT	DT-based method uses a DT to establish a model (i.e. a prediction model) to learn from training samples by representing them as branches and leaves. The pre-trained model is then used to predict the class of the new sample.	DT is a simple, easy-to-use and transparent method.	DT requires large storage because of its construction nature. Understanding DT-based methods is easy only if few DTs are involved.	Detection of intrusion [118, 119]and suspicious traffic sources
SVM	SVMs form a splitting hyperplane in the feature dimension of two or more classes such that the distance between the hyperplane and the most adjacent sample points of each class is maximised [21].	SVMs are known for their generalisation capability and suitability for data consisting of a large number of feature attributes but a small number of sample points	The optimal selection of a kernel is difficult. Understanding and interpreting SVM-based models are difficult.	Detection of intrusion , malware and attacks in smart grids
NB	NB calculates the posterior probability. It uses Bayes' theorem to forecast the probability that a particular feature set of unlabelled samples fits a specific label with the assumption of independence amongst features.	NB is known for its simplicity, ease of implementation, low training sample requirement [136] and robustness to irrelevant features (The features are preserved independently.).	NB handles features independently and thus cannot capture useful clues from the relationships and interactions among features. (It may work effectively in applications whose samples have dependent and related features.)	Detection of network intrusion
KNN	KNN classifies the new sample on the basis of the votes of the selected number of its nearest neighbours; i.e. KNN decides the class of unknown samples by the majority vote of its nearest neighbours.	KNN is a popular and effective ML method for intrusion detection.	The optimal *k* value usually varies from one dataset to another; therefore, determining the optimal value of *k* may be a challenging and time-consuming process.	Detection of intrusions and anomalies
RF	In an RF, several DTs are constructed and combined to acquire a precise and established prediction model for improved overall results.	RF is robust to over-fitting. RF bypasses feature selection and requires only a few input parameters.	RF is based on constructing several DTs; thus, it may be impractical in specific real-time applications in which the required training dataset is large.	Detection of intrusion [150], anomalies DDoS attacks and unauthorised IoT devices
AR algorithm	AR algorithms aim to study the relationship among the variables in a given training dataset *T* to discover correlations and consequently construct a model. This model is then used to predict the class of new samples.	AR algorithms are simple and easy to use.	The time complexity of the algorithms is high. AR algorithms use simple assumptions among variables (direct relationships and occurrence). In certain cases, these assumptions are inapplicable, especially to security applications.	Detection of intrusion
EL	EL combines the outputs of numerous basic classification methods to produce a collective output and consequently improve classification performance.	EL reduces variance and is robust to over-fitting. EL provides results beyond the original set of hypotheses; therefore, EL can adapt better than can a single classifier-based method to a problem.	The time complexity of an EL system is higher than that of a single classifier-based system.	Detection of intrusion, anomalies and malware
***k*-Means clustering**	*k*-Means clustering is an unsupervised learning approach that identifies clusters in the data according to feature similarities. *k* refers to the number of clusters to be generated by the algorithm.	Unsupervised algorithms are generally a good choice when generating the labelled data is difficult. *k*-Means clustering can be used for private data anonymisation in an IoT system because it does not require labelled data.	k-Means clustering is less effective than supervised learning methods, specifically in detecting known attacks	Sybil detection in industrial WSNs and private data anonymisation in an IoT system
PCA	PCA is a process that converts a number of probably correlated features into a reduced number of uncorrelated features, which are called principal components	PCA can achieve dimensionality reduction and consequently reduce the complexity of the model.	PCA is a feature-reduction method that should be used with other ML methods to establish an effective security approach.	PCA can be used for real-time detection systems in IoT environments by reducing the model features.

9.2 DL Approaches For The IoT Security

Recently, the application of DL to IoT systems has become one of the most critical areas of research. One of the main advantages of DL over traditional ML is its superior efficiency in handling large datasets.

Many IoT systems generate vast amounts of data; therefore, DL approaches are considered well-suited for these systems. Additionally, DL has the capability to automatically extract complex representations from raw data [40]. Deep learning approaches can also enable *deep linking* in IoT environments, which refers to a unified protocol that allows IoT-based devices and their applications to automatically interact with each other without human intervention [42].

For instance, IoT devices in a smart home environment can automatically interact to create a fully integrated smart home system. Deep learning approaches provide a computational model that integrates multiple processing layers to learn data representations at various levels of abstraction. Compared to traditional machine learning methods, deep learning has significantly advanced the performance of state-of-the-art applications [40].

Deep learning is a subfield of machine learning that employs multiple nonlinear processing layers for both generative and discriminative feature abstraction and transformation in pattern analysis. These methods are often referred to as hierarchical learning approaches because they can capture layered representations within deep architectures [41]. The working principle of deep learning is inspired by the structure and function of neurons and the human brain in signal processing. Deep networks can be built for supervised (i.e., discriminative) learning, unsupervised (i.e., generative) learning, or a combination of both, known as hybrid deep learning. Examples of supervised deep learning approaches include Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). Hybrid deep learning approaches include Deep Belief Networks (DBNs), deep Autoencoders (AEs), Generative Adversarial Networks (GANs), Restricted Boltzmann Machines (RBMs), and Ensembles of Deep Learning Networks (EDLNs) [41], [43].

Figure 7 explains Technological Tools That Fundamentally Enable the Deployment of ML/DL for IoT Security.

10. CONCLUSIONS

Since the Internet serves as the foundation for connecting IoT devices—enabling them to communicate, collect, and exchange information about our activities—it generates billions of gigabytes of data daily. By the end of 2025, it is expected that over 75 billion IoT devices will be connected globally. Naturally, as the number of these devices grows, so does the volume of data.This is where Artificial Intelligence (AI) plays a crucial role by bringing learning capabilities to the Internet of Things. However, a major drawback is the lack of robust security across many of these devices, which require the highest level of protection. The IoT is widely regarded as a global network of computing devices equipped with sensors and IP addresses that communicate over the internet. What makes security especially challenging in the IoT ecosystem is the diversity of devices. Many are designed to be low-cost and energy-efficient, and are often secured with only simple passwords. This makes them highly vulnerable to hacking attempts.

For this reason, many organizations are now incorporating AI into their security strategies, recognizing its vital role in protecting devices and data from potential attacks.AIoT will drive the evolution of existing IoT standards, paving the way for the development of autonomous future communication models that support intelligent data exchanges between millions of devices. This intelligence will enhance the state-of-the-art paradigms in network architectures.

Future research may focus on exploring the integration of AIoT with advanced applications such as smart health monitoring, intelligent transportation systems, energy-efficient smart grids, and personalized learning environments. This integration is expected to provide advantages such as real-time decision making, increased scalability, improved security, and sustainable resource management. Furthermore, identifying emerging trends such as edge AI, federated learning, and explainable AIoT systems will open up opportunities for developing reliable, transparent, and adaptable solutions across multiple domains.

11. REFERENCES

[1] Kok, et al., 2024. When IoT Meet LLMs: Applications and Challenges. In Proceedings of the International Conference on Big Data, IEEE.

[2] Yuan, P., 2024. Artificial intelligence in the Internet of Things: Integrating and optimizing AI algorithms for real-time data processing and decision-making. In Proceedings of the 2nd International Conference on Machine Learning and Automation.

[3] Dalhatu M., et al., Artificial Intelligence of Things (AIoT) for smart agriculture: A review of architectures, technologies and solutions. Journal of Network and Computer Applications, Elsevier, vol. 228, pp. 1-27, 2024.

[4] Sung, et al. 2021. Artificial Intelligence of Things (AIoT) Technologies and Applications. In Proceedings of the International Conference on Artificial Intelligence in Information and Communication.

[5] Sasan Z., et al. 2024. Joint Network Slicing, Routing, and in-Network Computing for Energy-Efficient 6G. In Proceedings of the Wireless Communications and Networking Conference, IEEE.

[6] Kim D., et al., Artificial Intelligence of Things (AIoT) Systems. Journal of Wiley Online Library, 2024.

[7] Revathy, R., et al. "Analysis of artificial intelligence of things." International Journal of Electrical Engineering and Technology 11.4 (2020).

[8] Ishengoma, Fredrick R., et al. "Integration of artificial intelligence of things (AIoT) in the public sector: drivers, barriers and future research agenda." Digital Policy, Regulation and Governance 24.5 (2022): 449-462.

[9] Elgazzar, Khalid, et al. "Revisiting the internet of things: New trends, opportunities and grand challenges." Frontiers in the Internet of Things 1 (2022): 1073780.

[10] Leong, Ying Mei, et al. "Transforming agriculture: Navigating the challenges and embracing the opportunities of artificial intelligence of things." 2023 IEEE International Conference on Agrosystem Engineering, Technology & Applications (AGRETA). IEEE, 2023.

[11] Era, Chowdhury Abida Anjum, Mahmudur Rahman, and Syada Tasmia Alvi. "Artificial intelligence of things (aiot) technologies, benefits and applications." 2024 4th international conference on emerging smart technologies and applications (eSmarTA). IEEE, 2024.

[12] Marinova, Natalia. "Advantages and ethical considerations of industrial iot artificial intelligence solutions usage." Бизнес управление 2 (2024): 43-58.

[13] Singh, Arun Kumar. "Smart Eco-Friendly Manufacturing System with Aiot Applications." Available at SSRN 4862891 (2024).

[14] Bronner W., et al. Sustainable AIoT: How Artificial Intelligence and the Internet of Things Affect Profit, People, and Planet. Connected Business. Springer, Cham, pp. 137-154, 2021.

[15] Kuguoglu BK., et al., The Giant Leap for Smart Cities: Scaling Up Smart City Artificial Intelligence of Things

(AIoT) Initiatives. Sustainability, vol.13, no.21, pp. 1-16, 2021.

[16] Calabrese M., et al., SOPHIA: An Event-Based IoT and Machine Learning Architecture for Predictive Maintenance in Industry 4.0. Information, Multidisciplinary Digital Publishing Institute, vol. 11, no.4, pp. 1-17, 2020.

[17] Juliet H., 2025. AI-Driven Predictive Maintenance for Industrial IoT with Real-Time Fault Detection and Prediction. In Proceedings of the 8th International Conference on Electronics, Materials Engineering & Nano-Technology, IEEE.

[18] D. Greenfield, How Siemens' Amberg Factory Uses Red Hat OpenShift. Automation World, Dec. 9, 2022. [Online].Available:www.automationworld.com/analytics/article/22591938/how-siemens-amberg-factory-uses-red-hat-openshift.

[19] Shen L., et al., 2025. AutoIOT: LLM-Driven Automated Natural Language Programming for AIoT Applications. In Proceedings of the The 31st Annual International Conference on Mobile Computing and Networking, Springer, Cham.

[20] Lee SM., et al., The Quality Management Ecosystem for Predictive Maintenance in the Industry 4.0 Era. International Journal of Quality Innovation, vol. 5, no.1, pp. 1-11, 2019.

[21] Mukhopadhyay SC., et al., Artificial Intelligence-Based Sensors for Next Generation IoT Applications: A Review. Sensors Journal, IEEE, vol. 21, no. 22, pp. 24920-24932, 2021.

[22] Pan Y., et al., Roles of Artificial Intelligence in Construction Engineering and Management: A Critical Review and Future Trends. Automation in Construction 122, Elsevier, vol. 122, pp. 1-21, 2021.

[23] Sharma V., et al., Optimal and Privacy-Aware Resource Management in AIoT Using Osmotic Computing. Transactions on Industrial Informatics, IEEE, vol. 18, no. 5, pp. 3377 – 3386, 2021.

[24] Lai H., et al., Study on Enhancing AIoT Computational Thinking Skills by Plot Image-Based VR. Interactive Learning Environments, vol. 29, no. 3, pp. 482-495, 2021.

[25] Tkachenko R., et al., An Approach Towards Increasing Prediction Accuracy for the Recovery of Missing IoT Data Based on the GRNN-SGTM Ensemble. Sensors, vol. 20, no.9, pp. 1-15, 2020.

[26] Karunakara L., et al., The Impact of Artificial Intelligence on the Modern Data Center Industry. International Journal of Advanced Research in Innovative Discoveries in Engineering and Applications, vol. 9, no. 4, pp. 19-38, 2024.

[27] Villar V., et al., Architectures for Industrial AIoT Applications. Sensors, vol. 24, no. 15, pp. 1-30, 2024.

[28] Revathy R., et al., Analysis of Artificial Intelligence of Things. International Journal of Electrical Engineering and Technology, vol. 11, no. 4, pp. 275-280, 2020.

[29] Caprotti F., et al., Platform Urbanism and the Chinese Smart City: the Co-Production and Territorialisation of Hangzhou City Brain. GeoJournal, Springer, pp. 1-15, 2020.

[30] Lee M., et al., 2020. Artificial Intelligence and Internet of Things for Robotic Disaster Response. In Proceedings of the International Conference on Advanced Robotics and Intelligent Systems, IEEE.

[31] Tsai Y., et al., Utilization of a Reinforcement Learning Algorithm for the Accurate Alignment of a Robotic Arm in a Complete Soft Fabric Shoe Tongues Automation Process. Journal of Manufacturing Systems, Elsevier, vol. 56, pp. 501-513, 2020.

[32] Lekkala S., et al., 2021 Emerging AI Security Threats for Autonomous Cars--Case Studies. Cornell University.

[33] Sun Z., et al., Artificial Intelligence of Things (AIoT) Enabled Virtual Shop Applications Using Self-Powered Sensor Enhanced Soft Robotic Manipulator. Advanced Science, vol. 8, no. 14, pp. 1-14, 2021.

[34] Cong L., et al., Internet of Things: Business Economics and Applications. Review of Business, vol. 41, no. 1, pp. 15-29, 2021.

[35] Faqishafyee N., et al., Mitigating Non-Technical Losses and Electricity Theft Through Smart Meters: A Case Study of the Akre District Power Distribution Network. Journal of Intelligent Systems and Control, vol. 3, no. 3, pp. 135-151, 2024.

[36] Abo-Zahhad M., An Embedded Smart System for Water Monitoring and Leakage Detection of Storage Tanks. Sohag Engineering Journal, vol. 3, no. 2, pp. 110-121, 2023.

[37] Tahsien S., et al., Machine Learning Based Solutions for Security of Internet of Things (IoT): A Survey. Journal of Network and Computer Applications, Elsevier, vol. 161, pp. 1-18, 2020.

[38] Ghaffari A., Securing Internet of Things Using Machine and Deep Learning Methods: A Survey. Cluster Computing, Springer, vol. 27, pp. 9065–9089, 2024.

[39] Deogirikar J., et al., 2017. Security Attacks in IoT: A Survey. In Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, IEEE.

[40] Al-Garadi M., et al., A survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. IEEE Communications Surveys & Tutorials, vol.22, no. 3, pp. 1646-1685, 2020.

[41] Zhang Y., et al., Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions. J. Artif. Intell. Res., Springer, vol. 75, no. 3, pp. 245–268, 2024.

[42] Chen J., Internet of Things (IoT) Authentication and Access Control by Hybrid Deep Learning Method - A Study. Journal of Soft Computing Paradigm, vol. 2, no. 4, pp. 236 - 245, 2021.

[43] LeCun Y., et al., Deep Learning. Nature, vol. 521, no. 7553, pp. 436-444, 2015.