Artificial Intelligence for IoT: Edge Computing, Security, and Applications

Seyed Mohammad Badzohreh
Tarbiat Modares University of Tehran

Abstract

The Internet of Things (IoT) has emerged as a fundamental component of the digital era, enabling seamless interconnectivity between billions of smart devices. By integrating physical and virtual entities, IoT extends the boundaries of technological ecosystems, generating vast amounts of real-time data. The efficient processing and analysis of this data are crucial for advancing IoT applications across various domains.

This survey provides a comprehensive review of the current state of IoT, exploring its fundamental concepts, key applications including smart healthcare, smart homes, intelligent transportation, and industrial automation and the underlying enabling technologies. Additionally, it examines critical challenges such as security, privacy, and scalability, alongside emerging solutions leveraging Artificial Intelligence (AI) and Deep Learning to enhance IoT capabilities.

By synthesizing existing research, this paper highlights prevailing trends, identifies open challenges, and outlines potential directions for future development. The insights presented aim to foster a deeper understanding of IoT's transformative potential and its convergence with next-generation technologies.

Keywords: Internet of Things, Security in IoT, Edge Computing, Artificial Intelligence, IoT Applications

Introduction

The Internet of Things (IoT) has emerged as a transformative technological paradigm, enabling seamless interconnectivity between billions of smart devices across various domains, including **smart cities**[1]**, healthcare, industrial automation, and intelligent transportation**[2]. This ecosystem integrates **physical and virtual environments**, facilitating **real-time data collection, exchange, and intelligent decision-making**. Fueled by advancements in **wireless communication, edge computing, and artificial intelligence (AI)**, IoT has become an essential component of modern digital infrastructure[3].

At its core, IoT consists of **sensor-enabled physical objects** that generate vast amounts of real-time data, requiring efficient management, processing, and analytics[4]. Traditional data processing techniques, while effective, often struggle to scale with the **increasing complexity, volume, and velocity** of IoT data. Consequently, **deep learning (DL)** has emerged as a powerful tool for analyzing IoT-generated data, offering enhanced capabilities in **pattern recognition, predictive analytics, and intelligent automation**[5]. By leveraging deep learning, IoT applications can **detect anomalies, optimize processes, and provide personalized user experiences** across diverse industries.

However, integrating deep learning with IoT introduces several **challenges**, including **resource constraints, security vulnerabilities, data heterogeneity, and real-time processing requirements**[6]. Many IoT devices operate in **resource-limited environments**[7], making it difficult to deploy complex deep learning models without efficient optimization techniques. Additionally, IoT networks are susceptible to **cyberattacks, adversarial manipulations, and data privacy concerns**[8], necessitating the development of **secure and explainable AI-driven solutions**.

This survey provides a **comprehensive review** of the convergence between IoT and deep learning, highlighting **key applications, architectural considerations, security challenges, and future research directions**. Specifically, this paper explores:

- The fundamental concepts and architectures of IoT, focusing on how deep learning enhances data-driven decision-making in connected environments.
- The role of deep learning in transforming IoT applications such as **smart healthcare, smart homes, autonomous transportation, and industrial automation**.
- The increasing need for secure and privacy-preserving IoT solutions, including deep learning-based threat detection and anomaly recognition.

- Emerging trends such as **federated learning, edge AI, and explainable AI**, which contribute to the next generation of intelligent IoT ecosystems[8].

By synthesizing existing research, this survey aims to provide **researchers, developers, and industry professionals** with valuable insights into **the current state, challenges, and potential advancements** in deep learning-driven IoT systems.

Classic Deep Learning Models

Recent advancements in deep learning have provided powerful tools for addressing the challenges and leveraging the opportunities presented by the vast amount of data generated in IoT environments. Deep learning models excel at automatically extracting intricate features from raw data, making them particularly suitable for complex tasks in various IoT applications. This section introduces fundamental deep learning models that have been widely employed in IoT systems.

- **Restricted Boltzmann Machines (RBMs)**

Restricted Boltzmann Machines (RBMs) are generative stochastic neural networks that learn a probability distribution over input data. They consist of a visible layer representing input features and a hidden layer that captures meaningful representations. RBMs can be stacked to form **Deep Belief Networks (DBNs)**, which enhance feature learning and dimensionality reduction[9]. These properties make RBMs particularly beneficial for handling high-dimensional sensor data in IoT applications, such as anomaly detection in industrial monitoring systems.

- **Autoencoders**

  Autoencoders are unsupervised neural networks designed to learn efficient, compressed representations of input data. They consist of an **encoder** that compresses the data and a **decoder** that reconstructs the original input from the compressed representation[10]. By forcing the network to capture essential patterns, autoencoders prove valuable in tasks such as **anomaly detection, data denoising, and feature extraction**, which are crucial for ensuring data reliability and security in IoT environments. For instance, autoencoders have been used in **intrusion detection systems** to identify malicious activity in IoT networks[11].

- **Convolutional Neural Networks (CNNs)**

  Convolutional Neural Networks (CNNs) are specialized deep learning architectures designed for processing grid-like data, such as images and time-series signals. They employ **convolutional layers** to automatically learn spatial hierarchies of features, making them highly effective in IoT applications, including:
  - **Image Recognition:** Used in smart home surveillance, industrial defect detection, and autonomous vehicles[12].
  - **Video Analysis:** Applied in **traffic monitoring** and **crowd analysis** for smart cities[13].
  - **Sensor Data Processing:** Helps analyze **wearable health monitoring data**, extracting patterns for disease prediction.

    Lightweight CNN architectures, such as **MobileNet and SqueezeNet**, are being explored for deployment on resource-constrained IoT devices, enabling real-time edge computing.
- **Recurrent Neural Networks (RNNs)**

  Recurrent Neural Networks (RNNs) are designed to process sequential data by maintaining a **hidden state** that captures temporal dependencies[14]. This capability makes them well-suited for time-series analysis in IoT applications, including:
  - **Predictive Analytics:** Used in **smart agriculture**, **weather forecasting**, and **energy consumption prediction**.
  - **Natural Language Processing (NLP):** Enables **voice-controlled IoT assistants** and **real-time speech translation** in smart devices.
  - **Deep Tracking:** Applied in **IoT-based surveillance systems** for real-time object tracking and movement analysis.

  Advanced variants, such as **Long Short-Term Memory (LSTM)** and **Gated Recurrent Units (GRU)**, address the vanishing gradient problem in traditional RNNs, making them more effective for long-term dependency tasks.
- **Transformer-Based Models (Emerging Trend)**

  While traditional RNNs have been widely used, the introduction of **Transformer models** (such as **BERT, GPT, and Vision Transformers (ViTs)**) has revolutionized deep learning in IoT. Transformers leverage

self-attention mechanisms to process data efficiently, leading to improved performance in NLP-based IoT systems and computer vision tasks[15].

Deep Learning-Based IoT Applications

The integration of deep learning with the Internet of Things (IoT) has led to the development of intelligent, adaptive, and efficient solutions across various domains. Deep learning models excel at processing vast amounts of sensor data, identifying complex patterns, and enabling predictive analytics, making them highly suitable for IoT-driven applications. This section explores recent advancements in deep learning-powered IoT across four key domains: **smart healthcare, smart homes, smart transportation, and smart industry**.

- **Smart Healthcare**
  The healthcare sector has witnessed a transformative impact through the convergence of deep learning and IoT. Key applications include:
  - **Health Monitoring:** Wearable devices and sensors enable continuous tracking of vital signs, such as heart rate, blood pressure, and glucose levels. Deep learning models analyze this real-time data to detect abnormalities and provide early warnings of potential health issues[16].
  - **Disease Diagnosis & Prediction:** Large-scale medical datasets, combined with deep learning algorithms, facilitate the prediction and diagnosis of diseases such as diabetes, cardiovascular conditions, and neurological disorders. For instance, **deep learning-based predictive models in healthcare big data clouds** enhance personalized diagnosis and treatment.
  - **Ubiquitous Healthcare Systems:** Cloud and edge computing enable **personalized telemedicine solutions**, allowing real-time monitoring and diagnostics in smart city healthcare infrastructures.

- **Smart Homes**
  Deep learning is playing a critical role in **enhancing automation, security, and personalization** in smart homes. Key applications include:
  - **Indoor Localization & Behavior Prediction:** AI-driven **indoor positioning systems** track the movements of occupants, optimizing energy usage and security.
  - **Intelligent Home Automation:** Smart assistants powered by deep learning learn user behavior, adjusting lighting, temperature, and appliance usage accordingly.
  - **Home Robotics:** Service robots use deep learning for **navigation, object recognition, and human-robot interaction**, improving assistance for elderly and disabled individuals[17].
  - **Gesture Recognition:** Deep learning enables **hands-free control of smart home devices**, improving accessibility and user experience[18].

- **Smart Transportation**
  The transportation sector is undergoing rapid transformation with IoT and deep learning integration. Key applications include:
  - **Traffic Prediction & Optimization:** Deep learning models analyze IoT sensor data from **vehicles, GPS, and cameras** to optimize traffic flow, reduce congestion, and improve travel efficiency.
  - **Traffic Monitoring & Safety:** IoT-enabled cameras, combined with **deep learning-based object detection and tracking**, enhance road safety by identifying traffic violations, pedestrian movements, and accident-prone areas[19].
  - **Autonomous Vehicles:** Deep learning is fundamental in **self-driving cars**, facilitating tasks such as **environment perception, decision-making, and control** based on data from LiDAR, cameras, and radar sensors[20].

- **Smart Industry (Industrial IoT – IIoT)**
  Deep learning and IoT are revolutionizing industrial automation, improving efficiency, safety, and predictive maintenance. Key applications include:
  - **Manufacturing Inspection:** AI-driven **visual inspection systems** detect defects in products using deep learning models trained on image and sensor data[21].
  - **Predictive Maintenance:** IoT-enabled sensors monitor equipment performance, while deep learning **predicts failures before they occur**, reducing downtime and improving resource allocation.
  - **Industrial Automation & Process Optimization:** Deep learning optimizes **supply chains, energy consumption, and robotic operations**, enhancing productivity and sustainability.

- **The Role of Edge Computing in IoT-Deep Learning Integration**
  Recent advancements in **edge computing** enable deep learning models to be deployed directly on IoT devices, reducing latency and ensuring **real-time decision-making** in resource-constrained environments[22]. This paradigm shift enhances **privacy, energy efficiency, and responsiveness** in applications such as autonomous driving, healthcare monitoring, and smart city infrastructure.

Challenges and Opportunities for Leveraging Deep Learning in IoT Applications

The integration of deep learning with the Internet of Things (IoT) offers significant potential to enhance automation, decision-making, and efficiency across various domains. However, this convergence also presents a unique set of challenges that must be addressed to fully unlock its capabilities. This section outlines key challenges and opportunities associated with leveraging deep learning in IoT applications.

Challenges

1. **Resource Constraints of IoT Devices**
   Many IoT devices operate under strict computational, memory, and power limitations. Deploying deep learning models on these resource-constrained devices is challenging due to the high computational demands of deep neural networks. Developing **lightweight architectures, model compression techniques, and efficient inference methods** is essential to ensure feasible deployment in real-world IoT settings.
2. **Massive Data Management and Processing**
   IoT systems generate vast volumes of data from distributed sensors, requiring **efficient storage, transmission, and real-time processing**. Managing and analyzing this massive data stream in a scalable and cost-effective manner remains a significant challenge. **Edge computing** offers a promising solution by processing data closer to the source, reducing latency and bandwidth consumption[23].
3. **Data Quality and Heterogeneity**
   IoT data is often **noisy, incomplete, and highly heterogeneous** due to variations in sensor types, environmental conditions, and transmission errors. Training robust deep learning models requires high-quality, well-annotated datasets, and **handling data inconsistencies and discrepancies remains a persistent challenge**.
4. **Security and Privacy Concerns**
   The pervasive nature of IoT devices raises critical **security and privacy issues**, as they collect and transmit vast amounts of sensitive personal and operational data. Furthermore, deep learning models are vulnerable to **adversarial attacks, data poisoning, and model inversion threats**. Ensuring the security of IoT systems and preserving data privacy during model training and inference is crucial[24].
5. **Real-Time Processing Requirements**
   Many IoT applications, such as **autonomous vehicles, industrial automation, and smart healthcare systems**, require **low-latency, high-speed data processing**. Ensuring that deep learning models deliver accurate, real-time predictions while operating on streaming data remains a major challenge.
6. **Interpretability and Explainability**
   Deep learning models often function as **black boxes**, making it difficult to interpret their decision-making processes. In critical applications such as healthcare, cybersecurity, and autonomous driving, model explainability is essential for **trust, accountability, and regulatory compliance**. Developing **explainable AI (XAI) techniques** for IoT applications is an ongoing area of research[25].

Opportunities

1. **Enhanced Data Analysis and Feature Extraction**
   Deep learning enables **automatic extraction of complex patterns** from raw IoT data, facilitating **more accurate predictions and intelligent decision-making**. This capability allows IoT applications to move beyond rule-based approaches toward **adaptive and data-driven intelligence**[26].
2. **Improved Automation and Control**
   Deep learning empowers **intelligent automation** in various IoT domains, including **smart homes, industrial robotics, and self-adaptive systems**. AI-driven control mechanisms enable **context-aware adjustments** in smart environments, optimizing resource consumption and enhancing user experience.
3. **Predictive Maintenance and Anomaly Detection**
   Deep learning models excel in **detecting anomalies and predicting failures** in IoT systems. By analyzing

sensor data from industrial machinery, vehicles, and critical infrastructure, AI-driven predictive maintenance reduces downtime, optimizes resource utilization, and enhances operational efficiency.

4. **Personalized and Context-Aware Services**
   IoT devices continuously capture **user behavior, preferences, and environmental conditions**. Deep learning can analyze this data to deliver **personalized recommendations and context-aware services**, enhancing applications in **smart healthcare, transportation, and home automation**.
5. **Enhanced Security and Threat Detection**
   Deep learning techniques can significantly improve **cybersecurity in IoT networks** by detecting **malware, intrusions, and network anomalies** in real time. AI-driven security mechanisms enhance **threat intelligence, fraud detection, and access control**, reducing vulnerabilities in IoT systems.
6. **Advancements in Edge Intelligence**
   The rise of **edge computing** and hardware accelerators enables **efficient deep learning inference on IoT devices**. This facilitates real-time analytics **without relying on cloud-based processing**, reducing latency and improving data privacy. Developments in **TinyML and federated learning** further support **decentralized intelligence** in resource-constrained IoT environments.

Overview of IoT System Architecture

The Internet of Things (IoT) is a complex ecosystem composed of interconnected smart devices, sensors, communication protocols, and computing infrastructures that collectively enable data-driven decision-making and automation. Understanding the architecture of IoT systems is crucial for designing and implementing deep learning-based solutions effectively. This section provides an overview of the fundamental components of IoT architecture.

Layers of IoT Architecture

A standard IoT system typically consists of three to five layers, each responsible for different tasks in data acquisition, processing, transmission, and decision-making.

1. **Perception Layer (Device Layer)**
   The perception layer comprises **sensors, actuators, and embedded devices** responsible for collecting real-world data. Sensors measure environmental parameters such as temperature, humidity, motion, and light, while actuators execute control actions based on received instructions[26].
2. **Network Layer (Communication Layer)**
   The network layer facilitates **data transmission** between IoT devices and cloud or edge computing infrastructures. Various **wireless and wired communication protocols**, such as Wi-Fi, Bluetooth, Zigbee, LoRaWAN, and 5G, play a critical role in ensuring reliable and low-latency data exchange[27].
3. **Edge Layer (Processing & Preprocessing)**
   The edge layer handles **local processing and filtering** of sensor data before transmission to cloud-based servers. Edge computing reduces network congestion and latency, enabling **real-time decision-making** for applications such as **autonomous vehicles and industrial automation**[28].
4. **Cloud Layer (Data Processing & Storage)**
   The cloud layer provides **scalable data storage, processing, and analytics capabilities** using **AI-driven cloud computing platforms**. Deep learning models are often deployed in this layer for large-scale analytics, anomaly detection, and predictive modeling[29].
5. **Application Layer**
   The application layer is the **end-user interface** that provides **data visualization, control, and decision-making functionalities**. Examples include **health monitoring dashboards, smart home control apps, and industrial process automation systems**[30].

Security Issues, Challenges, and Deep Learning-Based Mitigation Strategies in IoT Systems

The vast connectivity and heterogeneity of IoT systems expose them to a wide range of security threats, including cyberattacks, data breaches, and adversarial manipulations. Deep learning offers promising solutions for securing IoT infrastructures through intelligent threat detection and mitigation strategies.

Major Security Challenges in IoT

1. **Device Vulnerabilities**
   IoT devices often have limited **security capabilities**, making them susceptible to **malware, unauthorized access, and botnet attacks** (e.g., Mirai botnet).
2. **Data Privacy Risks**
   IoT networks handle vast amounts of **sensitive personal and operational data**, raising concerns about **data leaks, unauthorized surveillance, and compliance with regulations (e.g., GDPR, HIPAA)**[31].

3. **Adversarial Attacks on Deep Learning Models**
   Attackers can exploit **adversarial perturbations** to deceive deep learning-based security systems, leading to false predictions or misclassifications in applications such as **facial recognition and intrusion detection**[32].
4. **Network Attacks**
   IoT networks are vulnerable to **denial-of-service (DoS), man-in-the-middle (MITM), and eavesdropping attacks**, which can disrupt normal operations and compromise data integrity[33].

Deep Learning-Based Security Solutions for IoT

1. **Anomaly Detection Using Deep Autoencoders**
   Deep learning models, such as **autoencoders and variational autoencoders (VAEs)**, can detect unusual patterns in IoT traffic, identifying **anomalies, intrusions, and malicious activities** in real-time[34].
2. **Intrusion Detection Systems (IDS) with Convolutional and Recurrent Networks**
   - **CNN-based IDS**: CNNs can analyze network packet sequences to detect **malicious activities such as DDoS and phishing attempts**.
   - **RNN/LSTM-based IDS**: Recurrent neural networks (RNNs) and **long short-term memory (LSTM) models** are effective in detecting time-series-based threats, such as **botnet traffic and advanced persistent threats (APTs)**.
3. **Federated Learning for Privacy-Preserving IoT Security**
   - Traditional deep learning models require **centralized data storage**, which can pose **privacy risks**. **Federated learning** enables training models **locally on edge devices** while preserving data privacy, reducing exposure to cyber threats[35].
4. **Adversarial Defense Mechanisms**
   - **Adversarial training** involves **augmenting deep learning models** with adversarial examples to **improve robustness against attacks**.
   - **Defensive distillation** is another technique that helps **mitigate adversarial manipulations** in IoT security systems[36].

Future Research Directions

The convergence of IoT and deep learning presents numerous open challenges and research opportunities. Several promising directions for future exploration include:

1. **Energy-Efficient Deep Learning for IoT Devices**
   - Developing **lightweight neural networks (e.g., TinyML)** for **low-power, resource-constrained IoT devices**.
   - Exploring **quantization, pruning, and knowledge distillation techniques** to enhance model efficiency.
2. **Explainable AI (XAI) for IoT Applications**
   - Increasing transparency in **autonomous decision-making systems**.
   - Developing **interpretable deep learning models** for **mission-critical applications** such as **healthcare and autonomous driving**.
3. **Federated and Edge Intelligence for Secure IoT**
   - Enhancing **federated learning techniques** for **distributed, privacy-preserving model training**.
   - Designing **adaptive edge AI solutions** to reduce cloud dependency and **improve real-time analytics**.
4. **Robust Deep Learning Against Adversarial Attacks**
   - Strengthening **adversarial defense mechanisms** to enhance IoT security.
   - Investigating **blockchain-based security frameworks** for securing deep learning models deployed in IoT systems.
5. **Ethical Considerations and Regulatory Compliance**
   - Addressing **bias and fairness** in AI-driven IoT applications.
   - Ensuring **compliance with global data protection regulations (e.g., GDPR, CCPA)**.

Conclusion

The integration of deep learning with IoT is driving unprecedented advancements in automation, security, and real-time decision-making. However, scalability, privacy, security, and model interpretability remain critical challenges. This survey has provided a comprehensive overview of deep learning-based IoT applications, key challenges, and potential mitigation strategies.

Future research should focus on developing efficient and secure AI solutions for IoT systems, leveraging edge computing, federated learning, and adversarially robust deep learning architectures. Addressing these challenges will enable the next generation of intelligent, secure, and scalable IoT ecosystems.

References

[1] Alahi, M.E.E., Sukkuea, A., Tina, F.W., Nag, A., Kurdthongmee, W., Suwannarat, K. and Mukhopadhyay, S.C., 2023. Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: recent advancements and future trends. Sensors, 23(11), p.5206.

[2] Alahi, M.E.E., Sukkuea, A., Tina, F.W., Nag, A., Kurdthongmee, W., Suwannarat, K. and Mukhopadhyay, S.C., 2023. Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: recent advancements and future trends. Sensors, 23(11), p.5206.

[3] Xu, Z., Liu, W., Huang, J., Yang, C., Lu, J. and Tan, H., 2020. Artificial intelligence for securing IoT services in edge computing: a survey. Security and communication networks, 2020(1), p.8872586.

[4] Zheng, Y., Rajasegarar, S. and Leckie, C., 2015, April. Parking availability prediction for sensor-enabled car parks in smart cities. In 2015 IEEE tenth international conference on intelligent sensors, sensor networks and information processing (ISSNIP) (pp. 1-6). IEEE.

[5] Sarker, I.H., 2023. Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. Annals of Data Science, 10(6), pp.1473-1498.

[6] Malek, Y.N., Kharbouch, A., El Khoukhi, H., Bakhouya, M., De Florio, V., El Ouadghiri, D., Latré, S. and Blondia, C., 2017. On the use of IoT and big data technologies for real-time monitoring and data processing. Procedia computer science, 113, pp.429-434.

[7] Canavese, D., Mannella, L., Regano, L. and Basile, C., 2024. Security at the edge for resource-limited IoT devices. Sensors, 24(2), p.590.

[8] Arisdakessian, S., Wahab, O.A., Mourad, A., Otrok, H. and Guizani, M., 2022. A survey on IoT intrusion detection: Federated learning, game theory, social psychology, and explainable AI as future directions. IEEE Internet of Things Journal, 10(5), pp.4059-4092.

[9] Sarikaya, R., Hinton, G.E. and Deoras, A., 2014. Application of deep belief networks for natural language understanding. IEEE/ACM Transactions on Audio, Speech, and Language Processing, 22(4), pp.778-784.

[10] Bank, D., Koenigstein, N. and Giryes, R., 2023. Autoencoders. Machine learning for data science handbook: data mining and knowledge discovery handbook, pp.353-374.

[11] Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A. and Lloret, J., 2017. Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in iot. *Sensors*, *17*(9), p.1967.

[12] Rodriguez, M., Sridharlakshmi, N.R.B., Boinapalli, N.R., Allam, A.R. and Devarapu, K., 2020. Applying Convolutional Neural Networks for IoT Image Recognition. International Journal of Reciprocal Symmetry and Theoretical Physics, 7, pp.32-43.

[13] Wan, J., AAH Al-awlaqi, M., Li, M., O'Grady, M., Gu, X., Wang, J. and Cao, N., 2018. Wearable IoT enabled real-time health monitoring system. EURASIP Journal on Wireless Communications and Networking, 2018(1), pp.1-10.

[14] Ullah, I. and Mahmoud, Q.H., 2022. Design and development of RNN anomaly detection model for IoT networks. *IEEE Access*, *10*, pp.62722-62750.

[15] Wang, M., Yang, N. and Weng, N., 2023. Securing a smart home with a transformer-based iot intrusion detection system. *Electronics*, *12*(9), p.2100.

[16] Valsalan, P., Baomar, T.A.B. and Baabood, A.H.O., 2020. IoT based health monitoring system. *Journal of critical reviews*, *7*(4), pp.739-743.

[17] Roda-Sanchez, L., Olivares, T., Garrido-Hidalgo, C., de la Vara, J.L. and Fernandez-Caballero, A., 2021. Human-robot interaction in Industry 4.0 based on an Internet of Things real-time gesture control system. Integrated Computer-Aided Engineering, 28(2), pp.159-175.

[18] Hayashi, V.T. and Ruggiero, W.V., 2022. Hands-free authentication for virtual assistants with trusted IoT device and machine learning. Sensors, 22(4), p.1325.

[19] Xiao, Laisheng, and Zhengxia Wang. "Internet of things: A new application for intelligent traffic monitoring system." Journal of networks 6, no. 6 (2011): 887.

[20] Biswas, A. and Wang, H.C., 2023. Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain. Sensors, 23(4), p.1963.

[21] Li, L., Ota, K. and Dong, M., 2018. Deep learning for smart industry: Efficient manufacture inspection system with fog computing. IEEE Transactions on Industrial Informatics, 14(10), pp.4665-4673.

[22] Tien, J.M., 2017. Internet of things, real-time decision making, and artificial intelligence. Annals of Data Science, 4, pp.149-178.

[23] Yu, W., Liang, F., He, X., Hatcher, W.G., Lu, C., Lin, J. and Yang, X., 2017. A survey on the edge computing for the Internet of Things. IEEE access, 6, pp.6900-6919.

[24] Qian, C., Yu, W., Lu, C., Griffith, D. and Golmie, N., 2022. Toward generative adversarial networks for the industrial internet of things. IEEE Internet of Things Journal, 9(19), pp.19147-19159.

[25] Crabtree, A., Lodge, T., Colley, J., Greenhalgh, C., Glover, K., Haddadi, H., Amar, Y., Mortier, R., Li, Q., Moore, J. and Wang, L., 2018. Building accountability into the Internet of Things: the IoT Databox model. Journal of Reliable Intelligent Environments, 4, pp.39-55.

[26] Kumar, S., Sahoo, S., Mahapatra, A., Swain, A.K. and Mahapatra, K.K., 2017, December. Security enhancements to system on chip devices for IoT perception layer. In 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS) (pp. 151-156). IEEE.

[27] Al-Sarawi, S., Anbar, M., Alieyan, K. and Alzubaidi, M., 2017, May. Internet of Things (IoT) communication protocols. In 2017 8th International conference on information technology (ICIT) (pp. 685-690). IEEE.

[28] Sha, K., Errabelly, R., Wei, W., Yang, T.A. and Wang, Z., 2017, May. Edgesec: Design of an edge layer security service to enhance iot security. In 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC) (pp. 81-88). IEEE.

[29] Truong, H.L. and Dustdar, S., 2015. Principles for engineering IoT cloud systems. IEEE Cloud Computing, 2(2), pp.68-76.

[30] Hamid, H.G. and Alisa, Z.T., 2021. Survey on IoT application layer protocols. Indonesian Journal of Electrical Engineering and Computer Science, 21(3), pp.1663-1672.

[31] Nadikattu, A.K.R., 2018. IoT and the issue of data privacy. International Journal of Innovations in Engineering Research and Technology, 5(10), pp.23-26.

[32] Ibitoye, O., Shafiq, O. and Matrawy, A., 2019, December. Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks. In 2019 IEEE global communications conference (GLOBECOM) (pp. 1-6). IEEE.

[33] Pamarthi, S. and Narmadha, R., 2022. Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: network attacks and detection mechanisms. International Journal of Intelligent Unmanned Systems, 10(4), pp.482-506.

[34] Luo, T. and Nagarajan, S.G., 2018, May. Distributed anomaly detection using autoencoder neural networks in WSN for IoT. In 2018 ieee international conference on communications (icc) (pp. 1-6). IEEE.

[35] Li, J., Meng, Y., Ma, L., Du, S., Zhu, H., Pei, Q. and Shen, X., 2021. A federated learning based privacy-preserving smart healthcare system. IEEE Transactions on Industrial Informatics, 18(3).

[36] Singh, A. and Sikdar, B., 2021. Adversarial attack and defence strategies for deep-learning-based iot device classification techniques. IEEE Internet of Things Journal, 9(4), pp.2602-2613.