•

by . /ashish Ramana.

Submission date: 07-May-2024 10:52PM (UTC-0700)
Submission ID: 2374004605
File name: Ashish Ramana.docx (758.49K)
Word count: 5522
Character count: 30286

TERM PAPER

Topic:Integration of IoT with AI and ML

- Introduction:

Integrating IoT , AI and ML can be proves fruitful in many industries such as:

1. **Manufacturing:** Factories can install smart sensors on the machines . An alert on breakdown or service will be sent to the machine before it happens which will avoid inconveniencing the time which is lost when it needs an urgent service/repair. Intelligent systems can also enable businesses to create streamlined production lines, where machines are capable of performing complex tasks and improving productivity.

2. **Agriculture:** By sowing smart sensors in the soil area, these sensors will give the farmers information on moisture and crop health, which will enable the farmers to measure the level of water and fertilizer to apply. AI can be utilized to plant suitable crop for better earnings besides trying to forecast the weather

3. **Healthcare:** Doctors may analyze the patient's health data indirectly through smart wearables, which may deliver them to their electronic watch. AI is capable of examining medical scans and being able to use AI in more accurate diagnoses; moreover, the AI helps in an efficient way to determine the extent of the disease.

4. **Transportation:** AI and sensors are used by self-driving cars to make progress proximate and effortless by means of obstacle detection and path-finding. AI-traffic management can use traffic information to spot bottlenecks earlier which is an active way to address the pollution problem.AI can suggest best routes for smoother traffic flow, which are less crowded based on the traffic movements and the driving patterns.

5. **Retail:** AI can summarize customers' reviews to improve collection of products in store and to show only products they are interested in. The sensors and the various resourceful devices can be used to search extra products or deliver any product to customers.

- Literature Review:

Various Research papers along with the year,paper name,link of the paper,results & the algorithm used.

1. A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems

   This study was published in 2023 by the authors Hind Meziane and Noura Ouerdi. This study employed various ML techniques in order to build a big data architecture for the identification of intrusions in the IoT security network. The techniques employed included DNN, SVM, RF, DT, and NB. These methods were tested on the dataset of synchrophasor.

   The results showed that the DNN model produced the highest accuracy of 79.86%, which is not quite the 80% limit. The article provides a comparison table that summarizes the outcomes of various algorithms, the datasets used by each author, and the accuracy that was achieved. The survey, in addition to the aims of the allocations, datasets used, algorithms, and tasks that are treated such as classification (C), detection (D) and both classification and detection of intrusions, anomalies, or attacks (C-D).

   Finally, the DNN model had the highest accuracy among the techniques used in this experiment, but accuracy was not yet more than 80%. The paper presents a complete and thorough assessment by looking at the datasets, AI algorithms, and how precise they are.

2. The Role of AI in IoT Systems: A Semi-Systematic Literature Review.

   The study was carried out by Katambi Joan, Ivakale Anyonyi, Yvonne, in the year 2023. It was submitted as one of the requirements for M.Sc. in Computer Science at Lund University's Department, under supervision of Assoc. Prof. Romina Spalazzese. The thesis would come to an end in Spring Semester 2023.

   This thesis investigates the impact of artificial intelligence (AI) on Internet of Things (IoT) systems with a semi-systematic literature review that was supervised during the 2018- 2022 period. The investigation was carried out using special search conditions on the websites, like ACM Digital Library and Scopus, which information has been provided in various tables in the work. These tables provide a brief description of search methods, inclusion and exclusion criteria, quality assessment checklists, data extraction formats, and summaries on architectures, experiments, frameworks, reviews, cybersecurity, and cases involving application of artificial intelligence to internet of things systems.

   The thesis begins with a mention of the beneficiary of the Malmö University Master's Scholarship (MUMS) and the Swedish Institute, putting into the spotlight education's potential. The document also expresses appreciation to "Technology and Society: Malmö University Faculty" primarily the Department of Computer Science and Media Technology for providing assistance and their expertise imparted during author's study.

3. Sustainable Development through Machine Learning, AI and IoT.

This book is a collection of materials revised from the selected papers, which belong to the First International Conference on the Sustainable Development by the Means of Machine Learning, Artificial Intelligence and Internet of Things (ICSD 2023), held in Delhi, India on July 15-16, 2023. The book is edited by Pawan Whig, Nuno Silva, Ahmed A. Elngar, Negener Aneja and Pavika Sharma.

This book(a letterman jacket or a labor jacket), which is a part of the COMMSER series, contains 31 full papers. These papers were selected from 129 submissions. The papers are specifically addressing the inventions of ML, AI, and IoT technologies to have a great impact on green development. The paper overcomes the specific aspect of ML and AI as well as the range of approaches that are compatible with sustainable development projects.

Here fruit of this book will be food for researchers, practitioners and policy makers who work with sustainable development, containing recommendations on applying ML and AI successfully together with IoT in order to deal with numerous ecology and human-related challenges.

4. Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence.

This study published in 2023 in the journal PMC is titled "IoT Security Analysis: AI-Based Solutions for the Challenges Set Forth." The authors of the study are Mazhar, Dhani Bux Talpur, Tamara Al Shloul, Yazeed Yasin Ghadi, Inayatul Haq, Inam Ullah, Khmaies Ouahada, and Hebib Hamam.

The aim of this study is to examine the idea of using ML and DL in order to strengthen Internet of Things (IoT) device security. This research conducts analysis of the IoT security dataset to identify attack patterns from unstructured data, as an effort to prevent cyber-attacks happening in all the IoT devices.

ML and DL are aimed to detect the effective patterns that are the indicators of state of security breach in the IoT systems. The paper suggests a comprehensive security system which uses AI to reach a flexible and correct response to the threat level as it happens. Such a study sheds light on the advantages of deep learning caused by its capability to work with the complicated and fine-grained algorithms often involved in security attacks.

The end of the article stresses the fact that deep learning is a useful means to discover complicated patterns belonging to IoT security with influences on the resistance of IoT devices to the attack of cyberattacks.

5. IoT in the Era of Generative AI: Vision and Challenges.

The report was published on 2023, by authors Xin Wang, Zhongwei Wan, Arvin Hekmati, Mingyu Zong, Samiul Alam, Mi Zhang and Bhaskar Krishnamachari. This essay delves into AI generative technologies usage in the Internet of Things (IoT) environment.

The research puts into practice datasets from several IoT devices that serve as case studies of how Generative AI is applied. This topic is explored through the GenAI application to the Internet of Things (IoT) over the system's entire life cycle such as data generation, data processing, interfacing with IoT devices, and system development and evaluation.

The research results have revealed the huge prospects of AI Generative to upgrade the Internet of Things devices. The authors talk about the tremendous power Generative AI can possess in the evolution of IoT systems towards much higher degrees of efficiency, adaptability, and the management of complex operations such as self-healing and automated system design.

In conclusion, the article contends that Generative AI is a technology that holds great promise to enhance intelligent capabilities in IoT systems, allowing for performance and functional improvements of the systems.

6. Intelligent Machine Learning Based Internet of Things (IoT) Resource Allocation.

This article was published on 2023. The authors of this report are Koushik Chakraborty, Dhiraj Kapila, Sumit Kumar, Bhupati, Nazeer Shaik, and Akanksha Singh.

This research is about the implementation of machine learning (ML) methods for improving the resource utilization in IoT systems. The research is built on IoT resource data which is used through ML algorithm training and testing to boost resource distribution among the devices.

The main body of the paper comprises a new algorithm that takes IoT data-set parameters and produces optimum predictions for resource allocation to the end-users. The algorithm uses a fuzzy optimization methodology to place the IoT applications into classes partitioned into functional and nonfunctional properties in order to settle on resource allocation strategy.

In essence, it is shown that the application of ML to resource allocation in IoT has the efficiency and the effectiveness in managing the resources in the IoT environments. The findings show that the ML-powered intelligent systems can provide notable benefits such as more efficient resource consumption and improved operational performance.

7. Integration of Deep Learning into the IoT: A Survey of Techniques.

This article was published in 2023. The present study is of the authors Abdussalam Elhanashi, Pierpaolo Dini, Sergio Saponara, and Qinghe Zheng.

This paper survey gives a wide range of coverage about the use of deep neural networks to IOT applications. This discussion talks about the use of deep learning algorithms in the development of efficient and effective IoT systems. The study discusses the application of the IoT datasets through different domains, and emphasizes how deep learning plays its part in handling data generated by the devices IoT.

The authors pivot to examine the advantages of deep learning technology and apply it in the IoT domain, such as predictive maintenance, anomaly detection, and optimizing the resource allocation. Additionally, they look into how to do deep learning in IoT systems which have some implementation challenges, like, the need for large datasets, computational resources and energy efficiency.

As a result, it can be said that deep learning methods are providing notable increases in the efficiency of IoT applications. It suggests that in depth learning will allow for much more intelligent and autonomous applications of the IOT but it also ascertains that there are challenges that will have to be taken care of to realize these benefits in actual scenarios.

8. IoT Integration for Machine Learning System using Big Data Processing.

This article was published in 2024 in the International Journal of Intelligent Systems and Applications in Engineering. The authors of this study are Firas Tayseer Mohammad Ayasrah, Hala J. Abu-Al Nadi, Khaleel Al-Said, Gitanjali Shrivastava, G. Krishna Mohan, and Umesh Chandra.

This research explores the integration of machine learning (ML) techniques with big data processing within the context of the Internet of Things (IoT). The study utilizes a dataset comprising big data collected from various IoT devices, which provides a rich source of information for developing intelligent systems.

The core of the paper presents the application of ML algorithms to analyze and make data-driven decisions based on the vast amounts of data generated by IoT devices. The authors discuss the methodologies employed to process and analyze the data, emphasizing the potential of ML to enhance the efficiency and effectiveness of IoT systems.

In conclusion, the article demonstrates that the effective integration of ML with big data processing can significantly improve the capabilities of IoT systems. The research highlights the benefits of this integration, including improved decision-making and enhanced operational efficiency in IoT applications.

9. Smart cities: the role of Internet of Things and machine learning.

The article came out in 2023. The authors of the study are Amin Ullah, Syed Muhammad Anwar, Jianqiang Li. Lubna Nadeem, Tariq Mahmood, Amjad Rehman, and Tanzila Saba.

The paper is on integration of Internet of Things (IoT) and machine learning (ML) in the construction of smart cities. The paper uses the smart city data which involves various data obtained from urban surroundings so as to improve urban administration and service delivery.

The center of the paper describes how machine learning algorithms are used to process such data and to bring smart city applications into areas such as traffic management, energy distribution, public safety, and infrastructure maintenance. Smart city applications generate large-scale datasets that demand massive calculation and analysis processes to be utilized in due time.

The paper ends by stressing that machine learning enables smart city apps to function better than before. These technologies make it possible for analysts and decision-makers to make more data-driven decisions, which in turn lead to the creation of more liveable, sustainable and effective urban centers. The investigation also covers the problems of adopting these technologies in the lived neighborhoods but underlines their amazing transformative influence on urban development.

10. 11 Using Artificial Intelligence to Integrate Machine Learning,Fuzzy Logic, and The IoT as A Cybersecurity System.

    This 2023 study by Bansal et al. comprised of the authors Vipul Bansal, Ankit Bhardwaj, Jitendra Singh, Devvret Verma, Mohit Tiwari, Someshwar Siddi. The study promotes the integration of AI algorithms and fuzzy logic methods to increase the cyber security level of IoT devices.

    It applies different IoT security data sets monitored and evaluated using the proposed security solutions. Authors bring into discussion ML algorithms and fuzzy logic systems together with the purpose of IoT threat detection and mitigation in the environment.

    The results of the paper suggest an effective use of ML and fuzzy logic methods to enhance the safety of IoT networks. The authors are focusing on the advantages of this comprehensive approach which are e.g.: increased precision in threat detection, greater adaptability to changes in threats and better resources allocation.

    In the final part we will highlight that the united work of machine learning and fuzzy logic techniques has the most potent solution in the field of complexity of the IoT networks security problems. The research will help to intensify the need for more studies in the area and improve the security and reliability of IoT devices and networks.

11. 8 Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models.

This article was published in 2024 by author Fatima Alwahedi, Alyazia Aldhaheri, Mohamed Amine Ferrag and Ammar Battah. The research concentrates on using ML and generative AI technologies for the improvement of security of IoT instruments.

By using an IoT security dataset, the research was able to assess and evaluate the feasibility of the proposed security solutions. The author describes the existing machine learning powered security systems for the internet of things and how they can be enhanced by integrating generative AI and natural language processing.

The results of the study show that a method which uses a combination of ML and generative AI algorithms can dramatically improve the security of IoT systems. The authors emphasize the merits of the integrated approach and stress the main line of benefits such as enhanced threat detection, adaptability to unknown threats and better resource arrangement.

Briefly speaking, the article puts forward that generative AI and large language models are capable of solving complicated cyber security issues for IoT systems in an efficient manner. The study highlights the fact that the research should be continued in this area to have better security and reliability of the IoT devices and network.

12. The Interconnection of Internet of Things and Artificial Intelligence: A Review.

This article was written by the authors M H Gayantha, W.M.C. J.T. Kithulwatta, and R.M. Kapila Tharanga Rathnayaka in 2022. This research covers the case study of integration between IoT and AI technologies in detail.

Authors present a range of IoT and AI application-based datasets used in research projects to review the advantages and challenges of merging these two technologies in the studies. The review goes on to look at what algorithms and methods are being used for linking up IoT and AI systems.

The article ends with a note of how these technologies fit: IoT and AI together have the power to transform things in a meaningful way. Besides, the work proposes a few specific research gaps and sets forth different directions of development in the area of IoT-AI systems.

13. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches.

The research article has been published by the scholars (authors) Mahmudul Hasan, Md. Milon Islam, Md. Ishrak Islam Zarif, and M.M.A. Hashem in 2019. The work engages in the use of machine learning (ML) as a means of fortifying the security of Internet of Things sensors by discovering and stopping attacks and anomalies.

As the research uses a snapshot of several IoT sites, the performance of the proposed solutions is assessed and evaluated through analysis and examination of the dataset. The article talks about combining machine learning algorithms to stop intrusion and manage risks in cyberspace.

Because of the results of the study, the use of machine learning techniques, as the study has shown, can bring about significant improvement since the case of detecting attacks and anomalies to IoT sensors are effectively detected. The authors point out some advantages of such a method, such as better threat detection accuracy as well as years-long flexibility to constant changes.

Machine learning is the main tool for solving a range of security problems exposing connected IoT sensors. In the first place, it is more cost-effective than the conventional security means, since the involved operations are done repeatedly. It also addresses issues of scalability since, in the traditional ways, a monitoring source is used to provide security one time.

14. IoT and AI for Healthcare.

The article which was published in year 2022 is describing the work completed in 2022 by participating authors, Daoud and Otair This report entails research into (AI) and (ML) methods as hardware for enhancing the diagnostic precision of healthcare monitoring systems.

The study relies on data on healthcare monitoring to analyze and assess the accuracy of image pattern recognition algorithms through the diagnostic imaging. Authors deal with the combination of AI models to identify deviations in operational workflows and provide proactive alerts to the healthcare manpower.

The study has shown that the application of artificial intelligence systems induces the improvement of diagnostic accuracy of health monitoring systems. We see the advantage of this technique along with the improved ability of the systems in discovering anomalies, the advanced accuracy of detecting them and the ability of software for immediate alerting.

In summary, the paper demonstrates that AI and ML systems could be a viable solution for dealing with multifaceted issues within monitoring systems of healthcare provision and improve the amount of patients benefiting from these solutions.

15. AI-Enabled IoT Devices.

This article was published in 2024 but the content regarding to the study which was conducted in 2019 by Ahmed and Ali has been mentioned. The project considers the involvement of ML technologies in the improvement of functionality as well as the user interfaces of IoT gadgets.

Research exercises the device data usage for evaluation and analysis of machine learning algorithms performance. Authors talk about increasing utilization of ML to automate the task that

is repetitive or need not be done by the human and hence machine learning will be the future way of improving the efficiency of operation in IoT systems.

A summary of the findings indicates that the use of machine learning systems leads to notable improvements in the performance of the device and the user satisfaction level in relevant IoT systems. According to this method, the manufacturers and operators both are mainstreamed. This technique, however, ensures higher automation and also a better operational efficiency.

At the end, the paper underlines that machine learning is a perfect tool for tackling the many difficulties that the IoT systems may encounter and as a result, users gain higher degrees of satisfaction and devices work better.

16. Machine Learning Powered IoT for Smart Applications.

This article was released in the year 2021 by the authors of Hamad, Zhala Jameel, and Askar, Shavan. The research deals with implementing the deep learning methods for the increase of functionality of Internet of Things (IoT) systems and use for smart apps.

The data is drawn from deep learning datasets and processed to assess the effectiveness of deep learning algorithm in IoT systems. The authors speak of the contribution of deep learning to achieve the well-being of Internet of things systems in different smart areas.

The results of the study reveal that deep learning approaches can contribute immensely for smarter usage of IoT systems in various applications. Authors have addressed the advantages that this method carries, like increased automation, operational efficiency, and better user experience.

Concluding, deep learning is an impactful tool for increasing the performance and enhancing the user experience in smart devices applications brought about by the complex issues of IoT systems.

17. IoT Security and the role of AI/ML to Combat Emerging Cyber Threats in Cloud Computing.

This article was written in the year 2020 by co-authors Temechu G. Zewdie and the Anteneh Girma. The study concerns the implementation of the AI and ML methods at the cloud computing environment in order to improve security of the IoT gadgets.

The study builds on cloud network data to analyze and to assess the effectiveness of AI/ML algorithms that are designed to detect and counter cyber threats. In this paper, the integration of supervised, unsupervised, and reinforcement learning is discussed to enhance the security of IoT devices in the environments of cloud computing.

The research showed that a cyber security program based on AI/ML could effectively thwart emerging dangers in the IoT systems. This technique is discussed with special attention to the

benefits of such an approach — improved security, restricted devices and cloud resources access, secure ways to connect to the cloud, and device usage auditing.

In essence, the article highlights the role of the AI/ML models in making cloud computing IoT devices more secure, thus realizing the scope of the Internet of Things.

18. Micro energy harvesting for IoT platform.

This article was published in 2023 by authors Mahidur.R. Sarker, Amna Riaz, M.S. Hossain, Lipu, Mohamad Hanif Md Saad, Mohammad Nazir Ahmad, Rabiah Abdul Kadir, and José Luis Olazagoitia. The present study aims at employing AI based algorithms that are based on machine learning (ML) for energy management control of devices in the Internet of Things (IoT).

The completed study exploited IoT sensor data to monitor and examine AI-based algorithms for optimizing energy use and management. The writers talk about the utilization of AI so that the system gets an additional feature of monitoring the parameters of various systems. As a result, more power is saved by the IoT devices and the efficiency increases.

The outcome of the investigation is evident with the smart energy of AI algorithms which can intelligently manage the IoT devices. The authors state the advantages of such a method using examples of more system producing and preventing energy usage.

Therefore, this article focuses on the fact that AI based algorithms are among the new promising solutions for resolving the issues beyond the current IoT systems framework and finally increase the energy management for the present handheld devices in the markets.

19. Artificial intelligence in healthcare: transforming the practice of medicine.

This article was published in 2023 citing the authors: Junaid Bajwa, Usman Munir, Aditya Nori, and Bryan Williams. This paper concentrates on the use of AI in medicine in particular, it is applied in diagnostics and telehealth.

The research takes advantage of health care data for determining and examining the effectiveness of AI systems on accuracy diagnostics and distance diagnosis monitoring. Authors ground their discussion in the platforms and tools of AI to optimize the patient flow and patient experience, caregiver's experience, and patient safety.

As the study demonstrates, AI helps to combat inefficiency in the healthcare industry and optimize patient experience. The authors emphasize this method's benefits. For instance, it can help in early identification and telehealth care (e.g. smart wearables and sensors) of patients that may deteriorate.

At the end of the paper, it is clear that the use of AI technology in health service is a viable solution to some of the problems doctors are encountering and better results in the end.

19

20. Real-Time Analytics: Concepts, Architectures, and ML/AI.

This journal was published in 2023 by the authors Weisi Chen, Zoran Milosevic, Fethi A. Rabhi, and Andrew Berry. The study explores the utilization of AI and ML methods for near-time analytics in IoT applications.

The research employs IoT data in the process of analyzing and evaluating the efficiency of AI and ML algorithms applied in real time analytics. The authors will highlight the synergy of AI and ML in improving the performance and accuracy of IoT systems in different applications.

The research outcomes confirm that AI and ML techniques can significantly improve complex real-time analysis in IoT applications. The writers demonstrate the advantages of such method, for example greater automation, more effective operation and better user experience.

The paper ends by stressing the fact that AI and ML are some of the most effective solutions to the complex problems that IoT systems face and that as a result, device performance and user experience in real-time analytics will be greatly improved.

21. Artificial intelligence in customer relationship management.

This publication came out in 2022. The authors of the article were Cristina Ledro and Anna Nosella. The investigation aims at the integration of artificial intelligence (AI) in customer relationship management (CRM) to enhance customer engagement and satisfaction.

The research studies CRM data as a factor in its model performance assessment to improve the customer experience. The authors state that AI will be an essential part of their system to automate and personalize customer interaction processes, which will have positive effects on customer engagement and satisfaction.

The findings of this study suggest that AI has the potential to transform CRM systems by increasing customer interactions and improving user satisfaction. The writers bring to attention that this methodology is advantageous and it comes with increased automation, operation efficiency, and an improved user experience.

In summary, this paper focuses on the issue that the use of AI in CRM is a valuable solution for businesses. Through the improvement of customer relationships and business results, it, thus, overcomes the complex problems.

22. Integration of federated learning with IoT for smart cities applications

This article was released in the year 2023 by the authors Yazeed Yasin Ghadi, Tehseen Mazhar, Syed Faisal Abbas Shah, Inayatul Haq and Wasim Ahmad with Khmaies Ouahada and Habib Hamam named as co-authors. The research focuses on the hyper juxtaposition of deep learning and IoT in the field of smart city services.

The research applies the IoT data to evaluate and analyze the performance of deep learning algorithms, which are meant to be used in smart cities for the purpose of real-time tracking and predictive monitoring. Authors investigates the working principle of AI functions embedded in IoT Sensors through a deep learning accelerator that runs using software for AI training on mobile devices. This method is suitable in that it uses the hardware resources at their maximum efficiency for training data while maximizing overall performance and reliability.

The study shows that deep learning-based system makes possible a real-time monitoring and predictive maintenance in smart city for a number of applications. The authors emphasize the advantages of using a one-way model training model that reuses model outputs rather than model parameters which can, consequently, solve chat latency problems in IoT devices.

As for the conclusion, the article emphasizes the deep learning integration with IoT provides an opportunity for the solution of intricate problems faced by smart city applications consequently, the performance will be enhanced in real time monitoring and predictive maintenance.

- Objectives:

1. Establishing Technological Synergy

   A. Examine the Fundamentals: They should understand the core principles of AI, ML, and IoT, and also the roles that they play with one and another relationship.
   B. Explore Integration Mechanisms: Give a breakdown of how AI is the 'brain' of the IoT deployed devices which process and analyze the data making them 'smart'.

2. Doing the research on the Main Benefits and Applications of Field.

   A. Highlight Enhanced Efficiency and Automation: Describe how AI and ML works with IoT systems in the processes to simplify many complicated methods and increase the productivity of smart decisions to avoid human interruption.
   B. Explore Sector-specific Applications: Explore how the interrelation of industries such as healthcare, agriculture, industrial manufacturing, and smart cities is impacted by AIoT integration.

3. Getting rid of the obstacles and putting the solutions to the task.

A. Identify Integration Challenges: List the primary legal problems including data privacy, security, interoperability, and scalability during AIoT model deployment.
B. Discuss Potential Solutions: Determine the existing strategies and new technological breakthroughs that could be the best solutions to these problems.

4. Predicting Future Trends

A. Forecast Technological Advancements: Mirror the evolution of AI and ML, and their higher-level IoT applications, in terms of autonomy and intelligence.
B. Consider Economic Impacts: Evaluate the anticipated economic effects behind increasing scalability of AIoT, which may include efficiency gains and job transformation.

5. Ethics and societal issues.

A. Analyze Ethical Considerations: Discuss the ethical aspects of artificial intelligence in IoT including privacy issues, data ownership and decision making autonomy.
B. Evaluate Societal Impact: Consider how AIoT affects the dynamics of social interactions and how people's conducts get altered, particularly, privacy and safety.

6. Analyzing Scenarios and Practice.

A. Examine Successful Implementations: Give the concrete case studies of the AIoT solutions that were designed for particular sectors and that had been implemented in them. Show the strategies and the results that had been achieved.
B. Learn from Failures: Try to see through the cases in which the AIoT projects have been defective, elaborating the learnings and their application for the upcoming AIoT projects.

- Dataset Execution:

The executed data is collected from Kaggle which has temperature details from various times from the IoT devices. This dataset is taken and will perform a 7 day predictive temperature.

1. Reading the dataset

In [1]:

```
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.linear_model import LinearRegression
import matplotlib.pyplot as plt
from sklearn.metrics import mean_squared_error
from math import sqrt

# Load the dataset
# Change this to the path of your dataset
data = pd.read_csv("D:/SJU/SEM IV/Term Paper/IOT-temp.csv")

# Parse the noted_date column to datetime
data['noted_date'] = pd.to_datetime(data['noted_date'], format='%d-%m-%Y %H:%M')

# Check the first few rows of the dataframe
print(data.head())
```

```
                                id  room_id/id          noted_date  temp  \
0  __export__.temp_log_196134_bd201015  Room Admin 2018-12-08 09:30:00    29
1  __export__.temp_log_196131_7bca51bc  Room Admin 2018-12-08 09:30:00    29
2  __export__.temp_log_196127_522915e3  Room Admin 2018-12-08 09:29:00    41
3  __export__.temp_log_196128_be0919cf  Room Admin 2018-12-08 09:29:00    41
4  __export__.temp_log_196126_d30b72fb  Room Admin 2018-12-08 09:29:00    31

  out/in
0     In
1     In
2    Out
3    Out
4     In
```

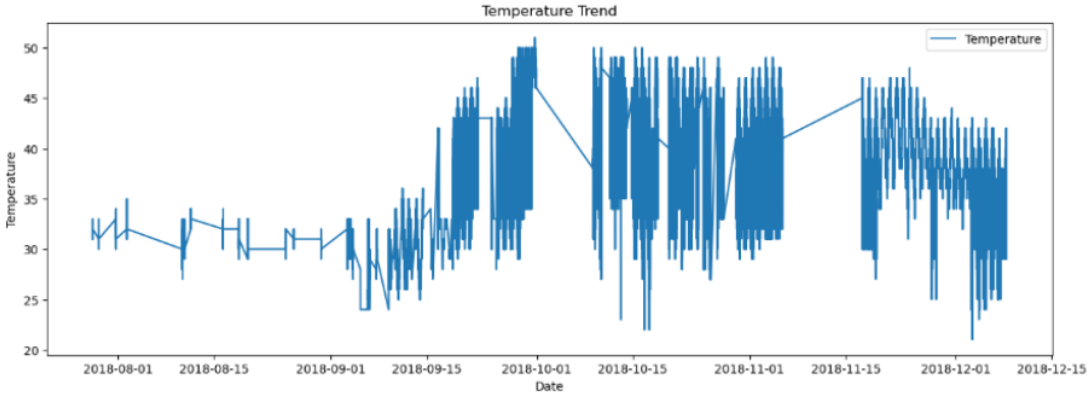
2. Plotting the temperature trend.

In [2]:

```
data['day_of_week'] = data['noted_date'].dt.dayofweek
data['hour'] = data['noted_date'].dt.hour
```

In [3]:

```
plt.figure(figsize=(15, 5))
plt.plot(data['noted_date'], data['temp'], label='Temperature')
plt.title('Temperature Trend')
plt.xlabel('Date')
plt.ylabel('Temperature')
plt.legend()
plt.show()
```



3. Feature Selection.

In [4]:
```
# Select features and target
X = data[['day_of_week', 'hour']]
y = data['temp']

# Split the data into training and testing sets
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)
```

In [5]:
```
model = LinearRegression()
model.fit(X_train, y_train)
```

Out[5]:

▾ LinearRegression

LinearRegression()

4. Y_pred & Mean Squared Error.

In [6]:
```
y_pred = model.predict(X_test)
rmse = sqrt(mean_squared_error(y_test, y_pred))
print(f'Root Mean Squared Error: {rmse}')
```

```
Root Mean Squared Error: 5.6273535519835605
```

5. Predict the next 7 Days temperatures.

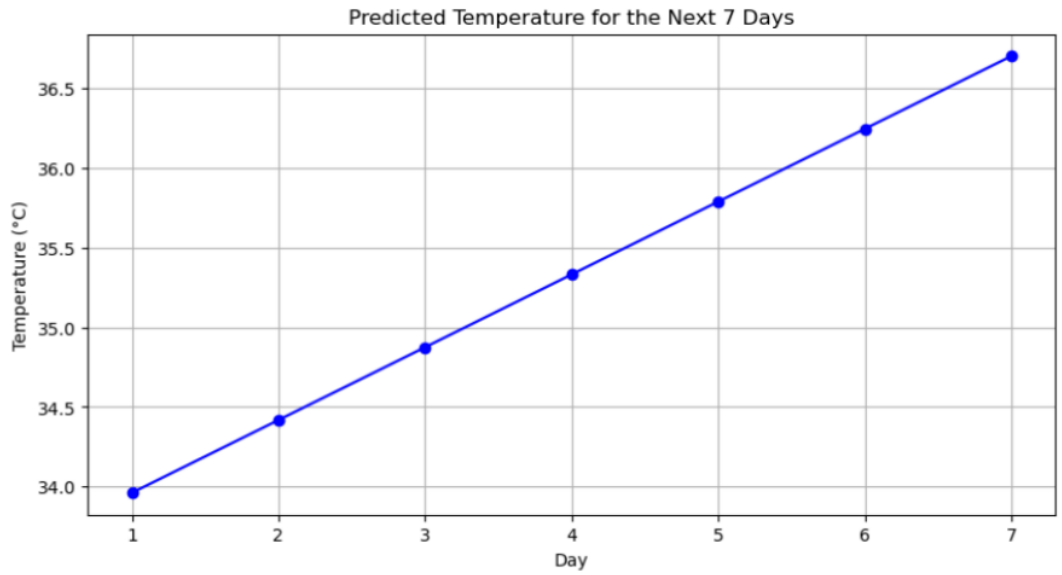
In [8]:
```
import numpy as np

# Assuming predictions for midday of upcoming days
future_days = np.array([[day, 12] for day in range(7)])  # Change '12' to any hour you want to pred
future_temps = model.predict(future_days)
print("Predicted temperatures for the next 7 days at noon:", future_temps)
```

```
Predicted temperatures for the next 7 days at noon: [33.96089171 34.41819483 34.87549795 35.3328010
6 35.79010418 36.2474073
 36.70471042]
```

6. Plot the predicted temperature.

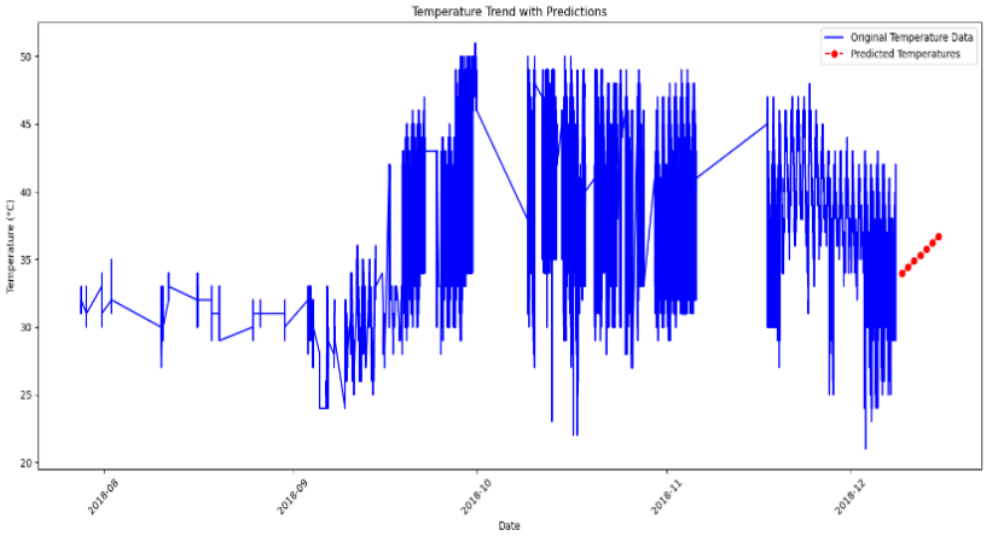
In [10]:

```
import matplotlib.pyplot as plt
import numpy as np

# Assuming 'future_temps' contains the predicted temperatures for the next 7 days
future_temps = [33.96089171,34.41819483,34.87549795,35.33280106,35.79010418,36.2474073
 ,36.70471042]  # Replace these values with your model's predictions

# Days for the x-axis
days = np.arange(1, 8)  # Representing the next 7 days

plt.figure(figsize=(10, 5))
plt.plot(days, future_temps, marker='o', linestyle='-', color='b')
plt.title('Predicted Temperature for the Next 7 Days')
plt.xlabel('Day')
plt.ylabel('Temperature (°C)')
plt.xticks(days)
plt.grid(True)
plt.show()
```



7.Plot Temperature Trend with Prediction

In [11]:
```
# Convert noted_date to datetime if not already done
data['noted_date'] = pd.to_datetime(data['noted_date'], format='%d-%m-%Y %H:%M')

# Sort the DataFrame by date to ensure correct plotting
data.sort_values('noted_date', inplace=True)

# Plot the original temperature data
plt.figure(figsize=(15, 7))
plt.plot(data['noted_date'], data['temp'], label='Original Temperature Data', color='blue')

# Assuming the last date in your dataset is the starting point for predictions
last_date = data['noted_date'].iloc[-1]

# Generate dates for the next 7 days
future_dates = [last_date + pd.Timedelta(days=i) for i in range(1, 8)]

# Plot the predicted temperatures
plt.plot(future_dates, future_temps, label='Predicted Temperatures', color='red', linestyle='--', ma

# Formatting the plot
plt.title('Temperature Trend with Predictions')
plt.xlabel('Date')
plt.ylabel('Temperature (°C)')
plt.xticks(rotation=45)
plt.legend()
plt.tight_layout()

# Display the plot
plt.show()
```



- Methodology
  1. Data Preprocessing
     A. Cleaning: The data will have to be given a thorough check in order to handle missing, duplicate as well irrelevant items among others. Temperatures entries are required to have the correct dates and the right readings for temperature for prediction.
     B. Normalization/Standardization: This may entail a specific kind of model used for the purpose of standardizing or normalizing temperatures to arrive at optimum points therein who I was initially skeptical of how this cooperation would turn out to be.

  2. Feature Engineering

     A. Timestamp Parsing: Dataset note the_date field is the timestamp corresponding to every monitor. Such visualization enables displaying vegetation index, which can be varied based on whether it is: hourly, daily or monthly value.
     B. Categorical Encoding: Internal/external area, and serving as an inside reading or an outside one, is a nominal variable to be transformed into a value of numbers suitable for machine learning algorithms that analyze data.

  3. Model Selection

     Due to the continuous nature of the temperature variable, regression models are the appropriate tool for this task.Potential algorithms could include:Due to the continuous nature of the temperature variable, regression models are the appropriate tool for this task.Potential algorithms could include:

     A. Linear Regression: The model serves as a good approach to get you started, but it is only effective and simple if the temperature is linearly proportional to the time of the day (otherwise other engineered features may separate the clusters).
     B. Random Forest Regressor: An ensemble that has the capacity to model more than simple linear relationships between features and response by simultaneously leveraging non-linear connections among attributes and response as well as adjusting its hyper-parameters without tuning extensively.
     C. Gradient Boosting Machines (GBM): Say for example, in the category of models XGBoost, LightGBM, or CatBoost, may be considered as perhaps they can handle different types of data through methods like gradient boosting technique to determine complex patterns.

  4. Modeling and metrics.

     A. Splitting the Dataset: The dataset will be cutted into training and testing sets to determine the model's accuracy for unknown cases.
     B. Cross-Validation: Additionally cross-validation such as k-fold might be required to test the model's robustness and to ensure that it doesn't get overtrained.

C. Performance Metrics: Metrics like MAPE, RMSE and R-squared will be used to check the model's accuracy and model performance.

5. Hyper parameter Tuning

Implementation of such approaches as grid search and random search to identify the ideal variable sets for the selected models is anticipated to increase the accuracy of these models.

6. Prediction and Analysis

A. Application of this method to train a new model in response to new data set or unseen data for projecting the future temperature values by including the features which were extracted from the original data.

Through analyzing the model's reading by it, we will understand the pattern, trends or deviations in the temperature readings.

.

ORIGINALITY REPORT

6%	6%	4%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.nature.com Internet Source	1%
2	www.mdpi.com Internet Source	1%
3	julib.fz-juelich.de Internet Source	1%
4	arxiv.org Internet Source	<1%
5	www.researchgate.net Internet Source	<1%
6	ouci.dntb.gov.ua Internet Source	<1%
7	"Sustainable Development through Machine Learning, AI and IoT", Springer Science and Business Media LLC, 2023 Publication	<1%
8	www.americaspg.com Internet Source	<1%

9	Douglas Montgomery, Steven Rigdon, Rong Pan, Laura Freeman. "Design of Experiments for Reliability Achievement", Wiley, 2022 Publication	<1 %
10	ijsrcseit.com Internet Source	<1 %
11	ieeexplore.ieee.org Internet Source	<1 %
12	www.essays.se Internet Source	<1 %
13	vixra.org Internet Source	<1 %
14	www.springerprofessional.de Internet Source	<1 %
15	www2.mdpi.com Internet Source	<1 %
16	doaj.org Internet Source	<1 %
17	jurnal.itscience.org Internet Source	<1 %
18	www.ijisae.org Internet Source	<1 %
19	deontik.com Internet Source	<1 %

20	Hind Meziane, Noura Ouerdi. "A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems", Scientific Reports, 2023 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		