ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 3 Issue 2 June 2023 / Page No: 101-109
Paper Id: JETA-V3I6P105 / Doi: 10.56472/25832646/JETA-V3I6P105

Review Paper

Recent Trends of Artificial Intelligence in the Internet of Things

Amitava Podder[1], Shyamalendu Paul[2]

[1,2]*Department of Computer Science & Engineering, Brainware University, Barasat, India*

Received Date: 14 June 2023 Revised Date: 23 June 2023 Accepted Date: 27 June 2023

Abstract: *The integration of Artificial Intelligence (AI) and the Internet of Things (IoT) is rapidly transforming various industries and enabling innovative applications. In recent years, several trends have emerged in the application of AI in the IoT, including edge computing for real-time analysis, predictive maintenance, intelligent automation, smart homes and cities, and security. Edge computing enables IoT devices to perform real-time analysis and decision-making, while predictive maintenance allows for proactive maintenance and reduces downtime. Intelligent automation enhances the efficiency and effectiveness of IoT devices, while smart homes and cities enable IoT devices to adapt to the needs and preferences of their users. Security is becoming a more significant concern, and AI can be used to detect and prevent cyberattacks. Overall, the integration of AI with IoT has the potential to create a more intelligent and efficient world, and we can expect to see even more innovative applications emerge in the future.*

Keywords: *Artificial Intelligence, Internet of Things, Internet of Everything, Intelligent Systems, Cyber-physical systems*

I. INTRODUCTION

The Internet of Things (IoT) and artificial intelligence (AI) are two quickly developing technologies that have the potential to completely change how we interact with technology. The Internet of Things (IoT) is the name given to the interconnected system of real-world items including machinery, cars, buildings, and other physical objects that have sensors, software, and network connectivity built into them. [2] These gadgets have the capacity to gather and exchange data, giving them knowledge of the outside world. The ability of robots to learn and carry out tasks that traditionally require human intelligence, such as speech recognition, picture analysis, and decision-making, is referred to as artificial intelligence (AI).

A more intelligent and effective world is being created because to the combination of AI and IoT. The use of edge computing for real-time analysis, predictive maintenance, intelligent automation, smart homes and cities, and security are just a few of the recent advances in the application of AI in the IoT. These developments are reshaping numerous industries and opening up new applications for IoT devices. We will delve deeper into these patterns in this post and talk about how they might affect technology in the future. [3].

Artificial Intelligence:

The ability of machines to carry out tasks that ordinarily require human intelligence, such as perception, thinking, learning, decision-making, and natural language processing, is known as artificial intelligence (AI). [6] Algorithms and statistical models are used to create artificial intelligence (AI), which enables computers to analyse and comprehend complex data, spot patterns, and make predictions based on that data.

There are various varieties of AI, such as:

A. Rule-based AI

This kind of AI bases its judgements on a predetermined set of rules.

B. Machine learning

This sort of AI makes use of algorithms to continuously enhance performance by learning from data.

C. Neural Networks

This sort of AI is made to recognise patterns in data by modelling its structure and operation after that of the human brain.

D. Deep learning

Deep neural networks with numerous layers are used in this branch of machine learning to analyse difficult data. Numerous industries, including healthcare, banking, transportation, and education, have used AI in some capacity. Image and speech recognition, virtual assistants, driverless vehicles, fraud detection, and predictive analytics are a few uses of AI. Concerns exist, though, regarding how AI might affect jobs, privacy, and security.

E. Intelligence

The ability of systems and devices to decide what to do and take the appropriate action based on information obtained from sensors and other sources is referred to as intelligence in AI and IoT. For instance, a smart thermostat may use information from occupancy and temperature sensors to modify a room's temperature automatically. In a similar manner, a smart security system may employ visual and audio sensors to identify intruders and notify the homeowner. [8]

The creation of systems that can learn from data and adjust to changing conditions is the main goal of intelligence in AI/IoT. The performance of the system can be enhanced over time by applying machine learning algorithms to analyse vast volumes of data from sensors and other sources. For instance, a smart energy management system may analyse energy usage data and optimise energy consumption patterns in a building using machine learning algorithms.

Recent developments in AI with IoT include edge computing systems, which move AI processing closer to the data source, and the application of blockchain technology to improve the security and transparency of IoT systems. A significant emphasis is also being placed on developing more intelligent and autonomous IoT devices and systems, such as drones and self-driving cars.

II. INTERNET OF THINGS

The Internet of Things (IoT) is a network of physical items, including machines, cars, buildings, and other physical objects, which are equipped with sensors, software, and connectivity to collect and exchange data online. From smartphones, smart household appliances, and wearable technology to commercial machinery and connected cars, this network of gadgets might consist of anything. [1]

In order to automate processes and increase efficiency, the IoT collects data from sensors that are built into these gadgets. For instance, a smart thermostat in a house might gather information on humidity and temperature and utilise that information to automatically modify the heating and cooling settings to save energy use. [5] Similar to this, a smart traffic management system might gather information on how the flow of traffic and utilise it to improve traffic signals and ease congestion.

Technology breakthroughs in areas like wireless networking, cloud computing, and big data analytics have made the IoT conceivable. These technologies allow for real-time processing and analysis of massive volumes of data as well as communication between devices and central systems.

The Internet of Things has a wide range of uses, including smart home automation, industrial automation, monitoring of healthcare, smart cities, and more. The IoT has the ability to change how we live and work by enabling us to make wiser decisions and automate more jobs than ever before as it grows and develops. However, there are also worries about how new technology may affect security and privacy, as well as the possibility of job displacement and other social and economic effects.

A. Internet of everything

In order to build a more connected, intelligent, and effective society, the Internet of Everything (IoE) concept, which is an extension of the Internet of objects (IoT) concept, envisions the integration of people, processes, data, and objects. The IoE broadens the IoT's focus from linking solely physical objects and gadgets to a wider spectrum of interconnected things, such as people, organisations, and processes.

By adding a layer of intelligence and analytics to the massive volumes of data created by connected devices, the IoE expands upon the basis of the IoT. The IoE can offer insights and suggestions that help organisations make better decisions and increase operational efficiency by analysing this data in real-time and using machine learning and other AI approaches.

Smart healthcare systems that use data from wearables and medical devices to monitor patient health and provide individualised treatments are examples of IoE applications. Smart cities that use data from sensors and other sources to optimise resource usage and enhance resident quality of life are other examples. Although the IoE is still in its infancy, it has the potential to profoundly alter the way we live and work. However, there are also worries about how new technology may affect security and privacy, as well as the possibility of job displacement and other social and economic effects. It will be crucial to address these issues as the IoE develops and make sure that this technology is used in a morally and responsibly manner.

B. Things and Everything

"Things" typically refers to actual physical things that have connectivity, software, and sensors integrated in them, enabling them to gather and exchange data online. This includes gadgets like mobile phones, jewellery, smart household appliances, and business machinery.

The term "everything," on the other hand, has a broader meaning and includes not just tangible items but also people, processes, and organisations. The idea of the Internet of Things (IoT) is expanded by the Internet of Everything (IoE) to encompass this wider spectrum of interconnected objects.

The IoE envisions a society in which everything is connected and integrated, with data flowing fluidly between people, processes, and things, in contrast to the IoT, which focuses on linking physical devices and items. This integration opens up new possibilities for efficiency and creativity, enabling businesses to make better decisions, streamline processes, and enhance the quality of people's lives.

However, this integration also creates fresh problems with regard to data ownership, privacy, and security. It is crucial to make sure that these technologies are used responsibly, ethically, and with the proper safeguards in place to protect people and organisations from possible hazards and abuses as more and more elements of our lives become online-connected.

C. AI Enabled IOT

AI-enabled IoT is the combination of Internet of Things (IoT) with artificial intelligence (AI) technologies to provide a more intelligent and effective network of interconnected devices. With the help of this integration, IoT devices can do more complex analytics, make more informed decisions, and automate processes beyond simple data gathering and exchange. [7]

The massive amounts of data created by IoT devices may be analysed using AI technologies like machine learning and natural language processing to find patterns and insights that would be difficult or impossible to find manually. Process optimisation, increased efficiency, and trouble prediction are all possible with this study.

AI-enabled IoT also gives devices the ability to learn and adjust in real-time to changing situations. To maximise comfort and energy efficiency, a smart heating and cooling system, for instance, may learn the preferences of a building's occupants and automatically alter the temperature and ventilation settings. [20]

Predictive maintenance for industrial equipment, intelligent traffic management systems, and individualised healthcare monitoring are more examples of AI-enabled IoT applications.

While there is great promise for the integration of AI and IoT to alter many aspects of our life, there are also significant ethical, privacy, and security concerns that are brought up. It will be crucial to make sure that these technologies are implemented responsibly and ethically, with the proper safeguards in place to protect people and organisations from possible hazards and abuses, as they continue to develop and become more pervasive.

There are numerous IoT applications that leverage AI, some of which include:

- Smart home automation: AI-enabled IoT gadgets can be used to automate and regulate a number of home features, including lighting, heating and cooling, security, and entertainment. A smart security system, for instance, can employ

machine learning algorithms to detect and address possible threats, while a smart thermostat can learn the preferences of the occupants and change the temperature accordingly.

- Predictive maintenance: AI-enabled IoT devices can be used to forecast when maintenance is required in sectors like manufacturing before a breakdown occurs. Machine learning algorithms can identify patterns and forecast when a component is likely to break by examining data from sensors on equipment. This enables maintenance to be planned in advance of the issue occurring.
- Smart agriculture: AI-enabled By keeping an eye on weather patterns, nutrient levels, and soil moisture, IoT devices can be utilised to optimise farming operations. The application of fertiliser and irrigation can be optimised using this information, increasing agricultural yields and lowering waste.
- Healthcare monitoring: AI-enabled IoT gadgets can be used to track patient health and deliver individualised care. For instance, wearables like fitness trackers and smartwatches can gather information on heart rate, sleep habits, and physical activity that can be used to monitor and manage chronic illnesses like diabetes and heart disease.
- Smart transportation: Traffic flow, congestion, and safety can all be improved with the help of AI-enabled IoT devices. In order to improve traffic signals and routing, for instance, sensors on roads and in moving vehicles can gather information about traffic patterns and road conditions.

These are just a handful of the numerous ways that the Internet of Things (IoT) with AI capabilities is affecting different sectors of the economy and parts of our daily life. We can anticipate seeing a lot more cutting-edge applications as these technologies develop further that will improve the productivity, convenience, and sustainability of our daily lives.

III. CYBER-PHYSICAL SYSTEMS

Cyber-physical systems (CPS) are systems that combine computational and communication technologies with physical components including sensors, actuators, and machines. CPS are intended to use digital technologies to monitor, regulate, and optimise physical processes. For many new applications, like smart cities, driverless vehicles, and Industry 4.0, CPS are a critical enabling technology. [12] These systems stand out from the competition by having the capacity to gather copious amounts of data from sensors and other physical components, analyse that data in real-time using machine learning and other AI approaches, and then use the knowledge obtained to improve system performance. CPS is used in a variety of systems, including those used in energy systems, industry, transportation, and healthcare. For instance, in smart cities, CPS are used to continuously monitor traffic flow, modify traffic signals, and improve the routes of public transportation. CPS are used in manufacturing to monitor and improve production processes, while they are used in healthcare to monitor patient health and give individualised care. [13] However, the fusion of physical systems with digital technologies also brings about fresh issues with regard to data ownership, privacy, and security. It will be crucial to make sure that CPS are implemented responsibly, ethically, and with the proper safeguards in place to protect people and organisations from possible hazards and abuses as they become more prevalent and complex.

A. CPS: A Combination of Disciplines

As the fusion of AI with IoT technologies enables the development of intelligent CPS, CPS are strongly tied to recent trends of AI in the Internet of Things (IoT). The development of intelligent CPS is made possible by the combination of AI and IoT technologies, which is why CPS are closely tied to current advancements in AI in the Internet of Things (IoT). A multidisciplinary approach integrating knowledge in computer science, control theory, electronics, mechanical engineering, data science, and artificial intelligence is necessary to design and execute AI-enabled CPS. As control theory provides the mathematical and engineering principles for designing and implementing control systems that can regulate physical processes, computer science provides the fundamental knowledge for designing and implementing software systems that can interact with physical components. Designing and constructing physical components like sensors, actuators, and machines requires expertise of both mechanical engineering and electronics. The processing and analysis of the massive volumes of data produced by IoT devices depend on data science and statistics, while real-time analysis and decision-making are made possible by AI and machine learning. [16] In addition to posing additional security, privacy, and data ownership issues, the combination of AI and IoT technologies also requires knowledge of cybersecurity and ethical principles.

As a result, the development of CPS is being driven by the recent trends of AI in the IoT, which call for a multidisciplinary approach, with specialists from other fields cooperating to design and execute these systems. To ensure that CPS are developed

and implemented in a way that maximises possible benefits while minimising risks and adverse effects, an interdisciplinary approach is crucial.

IV. COMPONENTS OF IOT-CPS

IoT-CPS's components are as follows:

- Physical Components: These are made up of tangible objects like sensors, actuators, and other devices that can interact with the environment and gather data from the outside world.
- Communication Networks: These are the networks that enable communication between devices and the cloud. Communication networks, which can be wired or wireless, can use a variety of protocols, such as Bluetooth, Wi-Fi, and cellular.
- Cloud Computing: This is a reference to the computer system that makes it possible to store, analyse, and analyse data produced by IoT-CPS. Big data analytics and machine learning can be used to glean insights from big datasets thanks to cloud computing.
- Edge Computing: This distributed computing paradigm enables data processing to take place closer to the point where the data is generated across the network. Edge computing can improve decision-making in real-time and reduce latency.
- Control Systems: These are the hardware and software components required for the management and control of physical processes using IoT-CPS. Physical processes can be regulated by control systems using feedforward control, feedback control, or a combination of the two.
- Artificial Intelligence: The massive datasets produced by IoT-CPS can be mined for insights using AI algorithms and techniques like machine learning and deep learning. The creation of predictive models and system performance optimisation can both be done with AI.
- Cybersecurity: It is crucial to make sure that IoT-CPS are secure and protected from online attacks as they become more widely used. Access control, authentication, and encryption are a few examples of cybersecurity measures.

The IoT-CPS's components cooperate to make it possible to gather, examine, and manage data from physical processes. This makes it possible to control physical systems more effectively and efficiently, which can enhance performance, save money, and have a smaller negative impact on the environment.

V. AI AND IOT-CPS

Since the combination of AI and IoT technologies enables the development of intelligent CPS that can learn and adapt to changing circumstances, AI and IoT-CPS are intimately tied to one another. The vast amounts of data produced by IoT devices may be analysed using AI algorithms and techniques like machine learning and deep learning to uncover insightful information. These discoveries can be applied to real-time decision-making, event prediction, and system performance optimisation. [9] For instance, in a smart manufacturing setting, sensors can be used to gather information on the operation of the machines and the output of the production process, and AI algorithms can then analyse that information to find patterns and abnormalities. By using this data to improve machine performance and decrease downtime, productivity and efficiency as a whole will increase. IoT sensors can be used in a smart city setting to track traffic flow, air quality, and noise levels. AI algorithms can then analyse this data to optimise traffic flow, lower pollution, and enhance inhabitants' quality of life in general. [10] Data security, privacy, and ethical issues are among the new concerns brought on by the combination of AI and IoT technology. As a result, it's critical to make sure AI and IoT-CPS are developed and implemented in a way that maximises potential benefits while reducing risks and adverse effects.

A. AI Enabled IOT-CPS

AI-enabled Artificial intelligence (AI) technology integration into IoT-CPS components is referred to as IoT-CPS. This integration makes it possible to develop intelligent CPS that are more effective and efficient because they can learn from their experiences and adjust to new circumstances. AI-enabled IoT-CPS analyses the massive volumes of data produced by IoT devices using AI algorithms and techniques like machine learning and deep learning. [11] These algorithms are capable of drawing out important information from the data, which may then be applied to real-time decision-making, event prediction, and system performance optimisation. IoT sensors, for instance, can be utilised in a smart healthcare setting to gather patient data like heart rate, blood pressure, and body temperature. The data can then be analysed by AI algorithms to look for trends and abnormalities that can point to a possible health issue. Healthcare experts can utilise this information to provide them an early warning and enable them to take proactive measures to avoid or treat the issue before it worsens. [12] IoT sensors can be utilised in a smart building environment to track energy use, temperature, and lighting conditions. The data can then be analysed by AI systems to

optimise energy use, cut expenses, and boost occupant comfort and productivity. A variety of industries, including manufacturing, transportation, and agriculture, will benefit from the combination of AI and IoT-CPS in terms of new prospects for innovation and disruption. But technology also brings along fresh difficulties in terms of data security, privacy, and moral considerations. Therefore, it's critical to make sure AI-enabled IoT-CPS are developed and implemented in a way that maximises potential advantages while reducing risks and adverse effects.

B. Cognitive AI and IOT-CPS

Artificial intelligence (AI) systems that can simulate human mental processes including learning, reasoning, and problem-solving are referred to as cognitive AI. Cognitive AI can be applied to IoT-CPS to allow intelligent decision-making and problem-solving skills, increasing the autonomy and effectiveness of IoT-CPS systems.

IoT-CPS systems with cognitive AI capabilities can learn from the data produced by IoT devices and base choices on that data intelligently. For instance, in a smart manufacturing setting, cognitive AI algorithms can examine data from sensors on production lines to find trends and abnormalities, and then modify the production process as necessary to improve productivity and decrease downtime.

[14] Similar to this, in a smart transportation setting, cognitive AI algorithms can examine information from IoT sensors on cars and roads to optimise traffic flow and reduce congestion, enhancing overall efficiency and cutting down on trip time. A variety of industries, including healthcare, agriculture, and energy, may see new potential for innovation and disruption as a result of the combination of cognitive AI with IoT-CPS.

[15] It also brings up fresh ethical and societal issues including bias, security, and data privacy. IoT-CPS and cognitive AI could revolutionise how we interact with and manage the physical environment, opening us new possibilities for productivity, efficiency, and sustainability. However, it's crucial to make sure that these systems are developed and implemented in an ethical and responsible manner, taking into account any potential effects on society and the environment.

C. Example cases of AI enabled IOT-CPS

IoT-CPS with AI capabilities are being used in a variety of sectors. Here are a few illustrations:

- Smart Agriculture: Crop growth may be monitored, and irrigation, fertilisation, and pest management can all be improved, using AI-enabled IoT-CPS. AI algorithms can analyse data collected by sensors on soil moisture, temperature, and nutrient levels to identify the ideal circumstances for plant growth and development. By adjusting irrigation and fertilisation rates, crop yields can be improved while using less water and fertiliser. [19]
- Smart Manufacturing: By tracking machine performance and anticipating maintenance requirements, AI-enabled IoT-CPS can be utilised to improve manufacturing operations. Machine vibrations, temperature, and other performance indicators can be measured using sensors, and AI systems can analyse the data to find trends and abnormalities. This information can be used to schedule maintenance in advance of when machines are expected to break, decreasing downtime and increasing overall productivity.
- Smart Healthcare: IoT-CPS with AI capabilities can be utilised to monitor patient health and enhance therapeutic results. Wearable sensors can be used to gather information on activity levels, vital signs, and other health parameters, and AI algorithms can then analyse that information to look for trends and abnormalities. [17] Healthcare practitioners can utilise this information to get an early warning and take preventative action to treat or prevent health issues before they worsen.
- Smart Cities: Traffic flow can be streamlined, pollution can be decreased, and city dwellers' general quality of life can be improved with AI-enabled IoT-CPS. AI systems can analyse the data from sensors that track traffic flow, air quality, and noise levels to improve efficiency and lessen pollution. In accordance with resident demands, this information may also be used to modify lighting and other city services.

IoT-CPS with AI capabilities has the potential to completely change how we interact with and manage the physical environment, opening up new possibilities for productivity, efficiency, and sustainability.

VI. CHALLENGES

The Internet of Things (IoT) ecosystem's adoption of artificial intelligence (AI) comes with a number of difficulties. These are a few of the principal difficulties:

- Data Privacy and Security: AI-enabled IoT systems produce a lot of data, some of it potentially sensitive. The security and protection of this data must be ensured against unauthorised access, cyberattacks, and breaches. Data encryption, secure storage methods, and secure communication protocols must be used for this.
- Interoperability and Standards: Standardisation of communication protocols and data formats is required due to the quick spread of IoT devices. Inefficient system behaviour and fragmentation might result from a lack of interoperability.
- Scalability: IoT systems produce a lot of data that must be analysed instantly. Designing and deploying AI-enabled IoT systems that can manage massive volumes of data and offer real-time insights presents a significant scalability challenge. [4]
- Energy Efficiency: Many IoT devices have limited battery life and must function for extended periods of time without being recharged. This necessitates the creation of AI algorithms with low power requirements that are also energy-efficient.
- Ethical and Social Considerations: IoT systems with AI capabilities have the potential to significantly alter society and the environment. It is crucial to make sure that these technologies are developed and implemented in a responsible and moral manner, taking into account any potential effects on social fairness, bias, privacy, and security. [18]
- Talent Gap: Professionals with knowledge of AI and IoT technologies are in short supply. Organisations may find it difficult to create and implement AI-enabled IoT solutions as a result.

A multidisciplinary approach that incorporates cooperation amongst specialists in AI, IoT, cybersecurity, and ethics is necessary to address these difficulties. To ensure the appropriate and long-term deployment of AI-enabled IoT systems, governments, business leaders, and academic institutions must collaborate to create standards and policies.

A. Challenges of CPS

Cyber-Physical Systems (CPS) are sophisticated systems that combine computing, networking, and physical components. While CPS have many uses and advantages across a range of industries, including manufacturing, healthcare, transportation, and smart cities, they also have a number of drawbacks. Here are some of the main difficulties CPS faces:

- Security: Because physical and cyber components are integrated in CPS, security is a significant concern. CPS are vulnerable to cyberattacks that take advantage of flaws in the connected systems, which can result in bodily injury, safety issues, privacy violations, and interruptions in crucial infrastructure. Strong authentication, encryption, intrusion detection, and resilient architectures are necessary for CPS security.
- Safety: The security of CPS is of utmost importance, especially when they are used in vital industries like healthcare and transportation. Risk management, failure prevention, and the implementation of fault tolerance and error recovery methods are all necessary for the safe operation of CPS. [21] Safety assurance can be a difficult undertaking due to the complexity of CPS because it necessitates incorporating safety considerations across the full system lifecycle.
- Interoperability and Integration: CPS frequently uses a variety of devices, protocols, and technologies from several manufacturers. It can be challenging to achieve seamless integration and interoperability across various parts, especially when working with legacy systems. To promote interoperability and simplify the integration of multiple CPS components, standardisation initiatives, open architectures, and clearly specified interfaces are crucial.
- Scalability and Complexity: Due of the numerous interrelated components, varied data sources, and changing surroundings, CPS can easily become very complex. [24] It gets increasingly difficult to manage the complexity as CPS deployments grow in size. To meet this problem, it is essential to design scalable CPS systems, create effective data processing and control algorithms, and control system dynamics.
- Privacy: CPS produce and handle enormous volumes of data, particularly sensitive and private data. It can be difficult to protect privacy while gaining useful insights from the data. To safeguard individual privacy in CPS deployments, it is crucial to ensure appropriate data anonymization, secure data transmission, access control measures, and compliance with privacy laws.
- Resilience and Reliability: To preserve their operation and performance, CPS should be able to resist failures, disturbances, and unfavourable circumstances. Redundancy, fault tolerance techniques, quick failure detection and

recovery, and reliable control algorithms are all necessary for developing resilient CPS. For critical applications, ensuring the dependability of CPS components and their interconnections is essential.

- Ethical and Legal Considerations: CPS bring up moral concerns about accountability, autonomy, and decision-making. Autonomous vehicles, for instance, are required to make split-second decisions that may affect human safety. Legal issues arise when determining responsibility and accountability in these situations. To solve these issues, ethical frameworks, legal requirements, and governance models must be established.

B. Challenges of IOT

A network of linked devices, sensors, and objects that can gather and exchange data is known as the Internet of Things (IoT). IoT has a number of opportunities for improving productivity, automation, and connectivity, but it also comes with a number of difficulties. Some of the major obstacles posed by IoT are listed below:

- Security: Due to the vast number of connected devices and the variety of their capabilities and weaknesses, security poses a big challenge in the IoT. Cybercriminals may target IoT devices in order to violate data privacy, get unauthorised access, or launch assaults. IoT devices are enticing targets because of weak authentication procedures, poor encryption, and a lack of security updates. To protect IoT systems, it's essential to include strong security measures like end-to-end encryption, secure protocols, and frequent firmware updates. [22]
- Privacy: IoT devices produce enormous volumes of data, often containing sensitive and personal data. These data's collection, processing, and storage present privacy issues. Personal data unauthorised access can result in identity theft, surveillance, and other privacy violations. [23] To address privacy issues in the IoT, it is crucial to put privacy-by-design principles, anonymization methods, data encryption, and user consent processes into practise.
- Interoperability and Standards: IoT involves a vast variety of hardware, software, and platforms from many vendors and industries. IoT device compatibility and interoperability issues might obstruct effective integration and communication. As a result, creating scalable and adaptable IoT ecosystems is challenging. To realise the full potential of IoT, it is essential to create common protocols, standards, and frameworks that provide interoperability and data exchange.
- Scalability and Network Management: IoT networks have the potential to quickly expand to encompass billions or perhaps more connected devices. Scalability problems include handling the tremendous volume of data created by IoT systems, managing such a vast number of devices, and guaranteeing dependable connectivity. To overcome scalability difficulties in IoT deployments, effective network management, data processing methods, and distributed designs are required.
- Power Consumption and Energy Efficiency: Many Internet of Things (IoT) devices have limited resources and rely on intermittent power sources, such batteries. As it directly affects the operating lifespan and maintenance needs of IoT devices, power consumption is a significant concern. The energy efficiency of IoT devices must be improved by optimising energy use, using low-power communication protocols, and creating energy harvesting strategies.
- Data Management and Analytics: Sensors, gadgets, and external systems are just a few of the many sources of data that the Internet of Things (IoT) creates. There are difficulties in efficiently managing, processing, and gaining useful insights from this data. To manage the complexity and amount of IoT data, scalable data management structures, real-time analytics, data quality assurance, and data storage are required.
- Ethical and Social Implications: Concerns about data privacy, surveillance, and the effect on human life are raised by IoT. Ethical conundrums may arise from the gathering and analysis of personal data, monitoring tools, and potential automation of crucial decision-making procedures. To solve these issues, it is essential to ensure openness, informed consent, and ethical standards in the design and implementation of IoT systems.

VII. CONCLUSION

In conclusion, the Internet of Things (IoT) ecosystem's integration of artificial intelligence (AI) has the potential to fundamentally alter how humans control and interact with the physical world. We can open up new prospects for efficiency, productivity, and sustainability across a variety of industries by fusing the strength of AI with the enormous volume of data produced by IoT devices. The integration of AI with IoT is not without its difficulties, though, including issues with data security and privacy, interoperability, standards, scalability, energy efficiency, ethical and social concerns, and the skill gap. A multidisciplinary approach that incorporates cooperation amongst specialists in AI, IoT, cybersecurity, and ethics is necessary to address these difficulties. Despite these difficulties, recent developments in AI and IoT are producing encouraging outcomes in fields including

smart cities, smart manufacturing, smart agriculture, and smart healthcare. We may anticipate seeing even more ground-breaking and significant use cases emerge in the years to come as AI and IoT technologies continue to develop and mature.

VIII. REFERENCES

[1] Evans D. The Internet of Things: how the next evolution of the internet is changing everything. Cisco Internet Business Solutions Group: Cisco; 2011.

[2] Lu Y, Xu LD. Internet of Things (IoT) cybersecurity research: a review of current research topics. IEEE Internet Things J. 2019;6(2):2103–15.

[3] Farivar F, Haghighi MS, Jolfaei A, Alazab M. Artifcial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT. IEEE Trans Ind Inf. 2020;16(4):2716–25. https://doi.org/10.1109/TII.2019.2956474.

[4] Vorakulpipat C, Rattanalerdnusorn E, Thaenkaew P, Hai HD. Recent challenges, trends, and concerns related to IoT security: aan evolutionary study. In: 2018 20th international conference on advanced communication technology (ICACT), Chuncheon-si Gangwon-do, Korea (South); 2018. p. 405–10.

[5] Linthicum D. App nirvana: when the internet of things meets the API economy. https://techbeacon.com/app-dev-testing/app-nirvana-wheninternet-things-meets-api-economy. Accessed 15 Nov 2019.

[6] Lakhani A. The role of artifcial intelligence in IoT and OT security. https://www.csoonline.com/article/3317836/the-role-of-artificial-intelligen ce-in-iot-and-ot-security.html. Accessed 11 Feb 2020.

[7] Roopak M, Yun Tian G, Chambers J. Models deep learning, for cyber security in IoT networks. In: IEEE 9th annual computing and communication workshop and conference (CCWC), Las Vegas, NV, USA. 2019;2019:0452–7.

[8] Radanliev P, De Roure D, Van Kleek M, Santos O, Ani U. Artifcial intelligence in cyber physical systems. AI & society. 2020; p. 1–14.

[9] Cañedo J, Skjellum A. Using machine learning to secure IoT systems. In: 2016 14th annual conference on privacy, security and trust (PST), Auckland; 2016. p. 219–22, https://doi.org/10.1109/PST.2016.7906930.

[10] Wang S, Qiao Z. Robust pervasive detection for adversarial samples of artifcial intelligence in IoT environments. IEEE Access. 2019;7:88693–704. https://doi.org/10.1109/ACCESS.2019.2919695.

[11] Pendse A. Transforming cybersecurity with AI and ML: view. https://ciso.economictimes.indiatimes.com/news/transforming-cybersecuritywith-ai-and-ml/67899197. Accessed 12 Feb 2020.

[12] Radanliev P, De Roure D, Page K, Nurse JR, Mantilla Montalvo R, Santos O, Maddox LT, Burnap P. Cyber risk at the edge: current and future trends on cyber risk analytics and artifcial intelligence in the industrial internet of things and industry 4.0 supply chains. Cybersecurity. 2020;3:1–21.

[13] Saptarshi Kumar Sarkar, Amitava Podder, Piyal Roy, 2023. *"An Analysis of the Privacy and Security Related Problem with Social Networks"* ESP Journal of Engineering & Technology Advancements 3(4): 37-43.

[14] Melamed T. An active man-in-the-middle attack on bluetooth smart devices. WIT Press, International Journal of Safety and Security Engineering. http://www.witpress.com/elibrary/sse-volumes/8/2/2120. Accessed 1 Feb 2018.

[15] Akram H, Dimitri K, Mohammed M. A comprehensive iot attacks survey based on a building-blocked reference mode. Int J Adv Comput Sci Appl. 2018. https://doi.org/10.14569/IJACSA.2018.090349.

[16] Biswas, S.K., Podder, A. (2022). Path Minimization Planning and Cost Estimation of Passive Optical Network Using Algorithm for Sub-optimal Deployment of Optical Fiber Cable. In: Mitra, M., Nasipuri, M., Kanjilal, M.R. (eds) Computational Advancement in Communication, Circuits and Systems. Lecture Notes in Electrical Engineering, vol 786. Springer, Singapore. https://doi.org/10.1007/978-981-16-4035-3_7

[17] Cekerevac Z, Dvorak Z, Prigoda L, Čekerevac P. Internet of things and the man-in-the-middle attacks–security and economic risks. Mest J. 2017;5:15–25. https://doi.org/10.12709/mest.05.05.02.03.

[18] Radanliev P, De Roure DC, Nurse JR, Montalvo RM, Cannady S, Santos O, Burnap P, Maple C. Future developments in standardisation of cyber risk in the Internet of Things (IoT). SN Appl Sci. 2020;2(2):169.

[19] Herberger C. DDoS fre & forget: PDoS—a permanent denial of service. Radware Blog, Radware Ltd. http://www.blog.radware.com/security/2015/10/ddos-fre-forget-pdos-a-permanent-denial-of-service/. Accessed 12 Sept 2016.

[20] Mode G, Calyam P, Hoque K. False data injection attacks in Internet of Things and deep learning enabled predictive analytics; 2019.

[21] De Donno M, Dragoni N, Giaretta A, Spognardi A. Analysis of DDoS-capable IoT malwares. In: 2017 federated conference on computer science and information systems (FedCSIS), Prague; 2017. p. 807–16. https://doi.org/10.15439/2017F288.

[22] Rouse M. What is IoT (Internet of Things) and how does it work? IoT Agenda, TechTarget. http://www.internetofthingsagenda.techtarget.com/ defnition/Internet-of-Things-IoT. Accessed 11 Feb 2020.

[23] Woo S. The right security for IoT: physical attacks and how to counter them. In: Minj VP, editor. Proft From IoT. http://www.iot.electronicsforu .com/headlines/the-right-security-for-iot-physical-attacks-and-how-to-counter-them/. Accessed 13 June 2019.

[24] Meneghello F, Calore M, Zucchetto D, Polese M, Zanella A. IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J. 2019;6(5):8182–201.