Intelligence of Things: Opportunities & Challenges

Hany F. Atlam[1, 2], Robert J. Walters[1], and Gary B. Wills[1]

[1]Electronic and Computer Science Dept., University of Southampton, Southampton, UK

[2]Computer Science and Engineering Dept., Faculty of Electronic Engineering, Menoufia University, Menoufia, Egypt

{hfa1g15, rjw5, gbw}@soton.ac.uk

Abstract— **The Internet of Things (IoT) is a promising technology that can connect and communicate virtual and physical objects globally. It allows billions of devices to be connected and communicate with each other to share information that creates new application and services. These services result in improving our quality of life. On the other hand, Artificial Intelligence (AI) is applied in many fields of science. It aims to understand techniques that require an intelligent action and solve complex problems. Integrating IoT with AI will create a powerful technology that can solve many of IoT problems that relate to the huge amount of data created by different IoT devices. With the huge analytic capabilities of AI, IoT data can be analysed efficiently to extract meaningful information. In addition, AI can help IoT devices to interact with humans and other objects intelligently and make autonomous decisions. This paper provides an overview of the integration of the IoT with AI by highlighting the integration benefits and opportunities of AI in different IoT applications. Challenges standing in the way of successful convergence of IoT with AI are also discussed. We can conclude that the integration of AI with IoT will generate a robust technology that can help companies to avoid unplanned downtime, increase operating efficiency, and enable new IoT applications and services.**

Keywords— Internet of Things, IoT, AI, Artificial Intelligence, Intelligence of Things.

I. INTRODUCTION

The Internet of Things (IoT) is a promising model that integrates several technologies and communication networks. It has the ability to connect and communicate worldwide virtual and physical objects through either wired or wireless networks. It is expected that by 2020, there will be more than 50 billion IoT objects [1].

The notion of IoT has been proposed by Kevin Ashton, who is the founder of MIT auto-identification centre in 1999 [2]. With the rapid growth and extensive applications of wireless sensor networks (WSNs) and cloud computing, the IoT has transferred from just a conceptual model to become a reality [3]. Nowadays, the IoT system has the capability to connect and communicate everyday objects over the Internet and enabling Machine-to-Human (M2H) and Machine-to-Machine (M2M) communication with the physical world. Current investments have been originated to solve IoT challenging research problems, develop and implement necessary standards of both software and hardware, and deploy the required infrastructure [4].

The next step is to integrate the Artificial Intelligence (AI) with the IoT to generate what is called "Intelligence of Things".

AI is progressively being used in humans' everyday life activities. The concept of AI is applied in many fields of science. It is playing a vital role in the research of management science and operational research areas. Intelligence is generally defined as the capability to collect knowledge to solve complex problems, while AI is the study and developments of intelligent machines and software that can reason, learn, gather knowledge, communicate, manipulate and perceive the objects [5]. Currently, intelligent machines replace humans in many areas such as welding and soldering of an assembly line, food preparation, and product packaging [4].

Integrating the IoT with AI will create a powerful technology that will have the ability to solve many of IoT problems that related to big data created from different IoT devices. It has been established that a large number of IoT devices generate a huge amount of data that need to be analysed to understand and extract meaningful information for use in different applications. It is expected that IoT devices will generate about 40 zettabytes (1ZB = 1million PB = 1billion TB = 1trillion GB) of data by the end of 2018 [6].

With the huge analytic capabilities of AI, many organizations are beginning to adopt AI approaches as a means of unlocking the value of large quantities of IoT data. This is because it can rapidly analyse massive amounts of IoT structured and unstructured data and give it a meaning by creating models of entities and concepts, and the relationships between them. They create hypotheses, formulate possible answers to questions, and provide predictions and recommendations, which can be used to support human intelligence and decision making [7]. AI approaches typically require a lot of processing power so, using these approaches directly with IoT devices often becomes impossible. Therefore, they are usually placed on external servers, which a user can use in the context of multiple devices at the same time [8].

This paper provides an overview of the integration of the IoT with AI. It starts by providing an overview of IoT and its layered architecture. IoT essential features are also discussed. In addition, the paper involves an examination of the benefits resulting from the integration process and IoT applications that will benefit from AI technologies. At the end, challenges standing in the way of successful convergence of the IoT with AI are also discussed.

The rest of the paper is organised as follows: Section II provides an overview of the IoT system; Section III discusses five layer architecture of the IoT; the essential characteristics of the IoT is presented in Section IV; Section V provides an overview of AI by presenting its essential features and different technologies; Section VI discusses the integration of the IoT with AI with showing benefits of the integration process; opportunities of AI in different IoT applications are discussed in Section VII; Section VIII presents challenges of the IoT with AI; and Section IX is the conclusion.

II. AN OVERVIEW OF IoT

The IoT has grown during the last few years to be able to connect billions of things globally. It can provide the connectivity to different things at anytime, anywhere, using any network path either through wired or wireless networks. These "things" have different capabilities, sizes, processing and computational power and can support different kinds of applications [9], [10].

The number of IoT devices is growing at a rapid rate. These devices can include personal computers, laptops, smartphones, tablets, PDAs and other hand-held embedded devices. Most of the mobile devices embed different sensors and actuators that can sense, and collect their surroundings, perform computation, make intelligent decisions, and transmit collected information over the Internet [11]

The IoT can be considered both a dynamic and global networked infrastructure that manages self-configuring objects in a highly intelligent way. This in turn, allows the interconnection of different IoT devices that share their information to create new applications and services which can improve human lives [12].

The concept of the IoT was first introduced by Kevin Ashton, who is the founder of MIT auto-identification centre in 1999 [2,12]. ITU has defined the IoT as "*a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies*" [14].

The IoT has incorporated in almost all our daily life applications and services, including smart home appliances, cars, mobile telephones, and others. These applications and services connect and communicate with each other to improve our lives in different ways [15].

III. IoT ARCHITECTURE

The typical layered architecture of the IoT is composed of five layers as shown in Fig.1.

The essential level is the perception layer (also called device or physical layer). This layer involves physical objects and sensor devices. There are many different sensors such as RFID, 2D-barcode, or Infrared sensors which depend on object identification techniques. Basically, the purpose of this layer is to identify different objects and collect environment information through sensor devices [12]. Different information can be collected by different types of sensors such as

temperature, motion, orientation, location, acceleration, humidity, chemical changes in the air, and others. The collected information is then transferred to the network layer to transmit it in a secure way to the information processing system [11].

The network layer is used to convey collected data securely from sensors to the information processing system. The data transfer can be done using either wired or wireless media by using a transmission technology such as 3G, UMTS, Wi-Fi, Bluetooth, infrared, or ZigBee. Therefore, the network layer aims to transfer the collected data from the perception layer to the middleware layer [16].

The middleware layer consists of a set of sub-layers that are used for the management of data, software, models, and platforms, and is located between the network layer and the application layer. The huge amount of data created and collected by IoT sensors is managed efficiently by Real-time Operational DataBase (RODB), which is also used for storing and management of models, knowledge, and other information [17]. Therefore, this layer receives the information from the network layer and stores it in the database. In addition, it performs information processing, ubiquitous computation and takes automatic decisions based on the results [12].
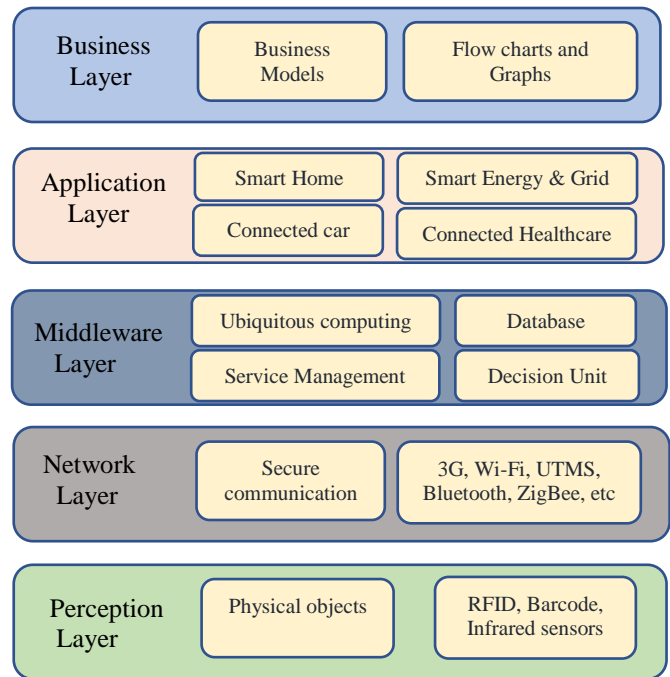

Fig.1. IoT reference layered architecture

The application layer provides global management of the applications that use the processed information of the middleware layer. It includes many IoT applications such as smart homes, connected cars, smart energy, connected healthcare, intelligent transportation and others [11].

The business layer is responsible for the management of whole IoT system including the applications and services. It generates business models, graphs, and flowcharts based on the data received from the application layer. The real success of the IoT technology depends on the appropriate business models

created through this layer. Based on the analysis of results, this layer will help to determine future actions and business strategies [11].

IV. ESSENTIAL CHARACTERISTICS OF IoT

The IoT is considered an emerging paradigm which consists of billions of uniquely addressable objects communicating with one another to form a global dynamic network [1]. It represents a promising future technology that shows some common characteristics as follows:

- *Dynamic environment*: IoT is a dynamic network in nature where objects are continually deployed; some new items joining the network while others leaving without determining network boundaries [18]. IoT devices can adapt to changing situations dynamically based on their operating conditions. For instance, surveillance cameras can change their modes based on whether it is day or night. Cameras could switch from lower resolution to higher resolution modes when motion is detected and alert nearby cameras to do the same [19].

- *Large scale***:** There are billions of IoT devices. These devices need to be managed to enable them to communicate with each other. The data generated by them and its interpretation for application purposes are also critical [20].

- *Sensing*: IoT could not be realized without sensors. Sensors are used to perceive changes in the environment to generate data that reflect their status or even interact with the environment. Sensing technologies provide capabilities that reflect the awareness of humans and physical world. Although the sensing information may be just the analogue input from the physical world, it can deliver a good understanding of our complex environment [14].

- *Intelligence*: With the integration of software algorithms and hardware, IoT devices become smart. These capabilities permit IoT devices to interact in an intelligent way in certain situations. Although the popularity of smart technologies, intelligence in the IoT is only means of interaction between devices, while user and device interactions are achieved by usual input methods and graphical user interfaces [21].

- *Massive amount of data*: There are billions of IoT devices which create a large amount of data which raises many issues including those related to security and privacy [21].

- *Heterogeneity*: The IoT system involves different devices, platforms, operating systems, and services which are connected with each other using different protocols [14].

- *Connectivity*: Connectivity enables network accessibility and compatibility. It empowers the IoT by bringing together everyday objects. It also provides new market opportunities for IoT that can be created by the networking of smart things and applications [22].

V. ARTIFICIAL INTELLIGENCE

According to the Merriam-Webster dictionary, AI is defined as the capability of a machine to imitate intelligent human behaviour. AI was launched officially as a discipline in 1956 at a Dartmouth College conference by John McCarthy, Marvin Minsky, Allen Newell, and Herbert Simon [23]. The main purpose of AI is to recognize the principles and mechanisms that need an intelligent action and provide the solution to complex problems at high levels of competence [22].

The significant challenge of AI is to build models and mechanisms that produce an intelligent action. AI is mainly an experimental science, in which researchers use the conventional hypothesis-and-test research model to test and confirm these models and mechanisms. The computer is considered as the main laboratory where AI experimentations are carried out. AI researchers confirm hypotheses by testing and validation of computer programs [23].

There are many areas and applications that use AI such as expert systems, robotics and sensory systems, natural language processing, speech understanding, intelligent computer-aided instruction, computer vision and scene recognition, neural computing, and others [7]. Some areas and applications of AI can be seen in Fig.2.
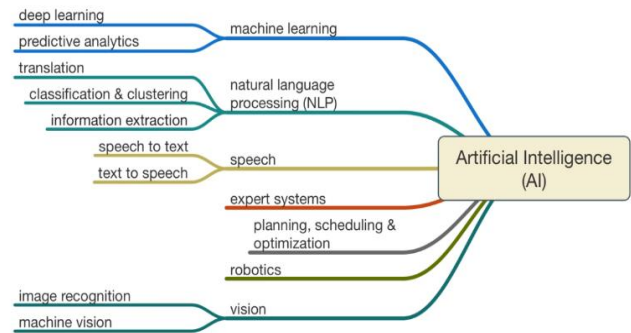

Fig.2. Areas and applications of AI

According to Reddy and Minsky [23], the characteristics of an intelligent system include:

- Showing adaptive goal-oriented behaviour
- Learning from previous experience
- Use of enormous amounts of knowledge
- Showing self-awareness
- Interacting directly with humans using language and speech
- Tolerance of errors and ambiguity in communication
- Responding in real time.

AI is different from computer science as it focuses on perception, reasoning, and action. It makes machines smarter with the help of artificial neurons and scientific theorems [5].

VI. IoT with AI

The IoT consists of virtual and physical objects, sensors, actuators, services, and applications that have unique identifiers [24]. It is incorporated in many applications of our life such as agriculture, remote patient monitoring, driverless cars, smart grids, smart cities, and smart home appliances.

The IoT is referred as the driver of the fourth industrial revolution. It has generated technological changes that extend to a wide range of applications. Cisco predicted that by 2020, there will be more than 50 billion of connected things worldwide [25]. The IoT growth brings huge chances to make our lives easier with enhancing efficiency, productivity, and safety of many business applications [25].

With the rapid increase of IoT devices, the data collected by these devices will present a new challenge of how to analyse this huge amount of data. Collecting this data will not be beneficial to anyone unless there is a way to analyse and understand it. As shown in Fig. 3, International Data Corporation (IDC) has predicted that by 2025, the total number of data created by IoT devices will reach about 180 zettabytes. This growth comes from both the number of devices generating data as well as the number of sensors in each device [26].
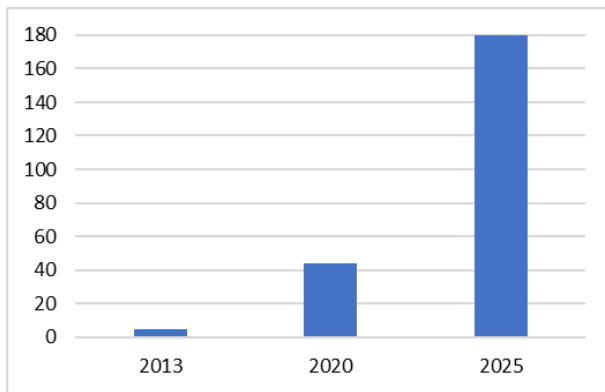

Fig. 3. Expected data generated by IoT devices in Zettabytes

With the analytic capabilities of AI, IoT data can be analysed and different organizations can classify and understand patterns and make more informed decisions [27]. As shown in Fig. 4, IoT generates and collects a huge amount of data that for analysis and meaningful information extracted using AI approaches.
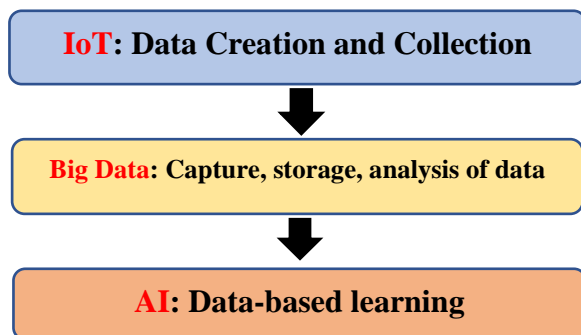

Fig. 4. AI plays a vital role in analysing big data created by IoT devices.

AI is playing a growing role in IoT applications and deployments. It is the driver that will allow analytics and decision making from the data collected by IoT devices. AI brings the ability to identify patterns and differences in data that different IoT devices generate such as temperature, humidity, pressure, air quality, and sound [7].

Using the power of AI with the huge amount of IoT data will lead to full benefits of IoT data, which will lead to a diversity of benefits for both customers and companies such as proactive intervention, intelligent automation, and highly personalised experiences. It also allows us to define new ways for IoT connected devices to work together better and make these systems easier to use [7]. In addition, AI can deliver programmatic reasoning, self-correction, and ultimate learning. It can manage the huge amount of data created by IoT devices by delivering a seamless customer experience [17].
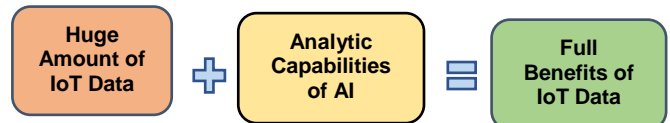

Fig. 5. Integrating AI with IoT will get full benefits of IoT big data

VII. OPPORTUNITIES OF AI IN IoT APPLICATIONS

The convergence of AI with IoT will bring unlimited benefits to many of IoT application. These applications can include:

1. *Aircraft*: aircraft contain many sensors that continuously monitor the status of various systems and sub-systems to identify existing faults and predict future faults and their degree of severity. Applying AI on these huge collected data will result in higher safety and lower aircraft delays or downtime [28].

2. *Connected and Remote Operations*: With smart and connected warehouse operations, workforces no longer have to wait for the warehouse to pick goods off the shelves to fulfil an order. Instead, shelves whisk down the passages, guided by small robotic platforms that deliver the right inventory to the right place, avoiding collisions along the way. Order fulfilment is faster, safer, and more efficient [27].

3. *Smart buildings*: Smart sensors connected to buildings can significantly increase safety by reducing risks such as fire and flooding, while also decreasing operational costs, and improving energy efficiency by AI capabilities. For instance, monitoring the movement of people around the building and adjusting temperatures accordingly [28].

4. *Healthcare*: This is an application of IoT that attracts the attention of many organizations. Smart sensors can monitor various bodily activities to improve safety and maintain health. Devices can monitor people's activity levels and help to change their behaviours to improve well-being, while medical sensors can support overall health, for example, by monitoring blood sugar levels and dispensing insulin when necessary [5].

5. ***Maintenance***: Large manufacturing and industrial companies are empowering their machinery with sensors to carry out predictive maintenance and autonomously identify faults that may happen in the future. For example, companies that wanted to reduce machinery breakdowns without increasing its maintenance costs [23].

6. ***Cognitive systems:*** IoT with machine learning can be tremendously valuable in shaping our environment according to our personal preferences. It will create new methods that appeal to the user's sense of taste, creating optimized menus for each individual, and automatically adapting to local ingredients [27]. For example, Nest Thermostat uses machine learning to learn customer/owner preferences for heating and cooling and ensuring that the house is at the preferred temperature when the owner gets home from work or when they wake up in the morning [27].

VIII. CHALLENGES OF IoT WITH AI

Although the integration of AI with IoT will bring many benefits that can increase IoT data efficiency, there are many challenges that stand in the way of successful convergence of IoT with AI. These challenges include:

1. ***Complexity***: IoT is a complicated system as it has billions of devices. Therefore, performing operations with this large scale of objects/things makes the coordination process very complex. Integrating AI with this complex system will not be an easy task as it requires taking into account different IoT constraints like processing power, memory, and delay in real time applications [29].

2. ***Heterogeneity***: The IoT interconnects large numbers of devices/objects to provide new applications that improve our quality of life. However, one of the important challenges faced by the IoT systems is the wide heterogeneity of devices, platforms, operating systems, and services that exist and might be used to create new applications [30]. As the IoT continues to grow, the need for services that work with multiple IoT applications will need to continue to increase to realize the promised efficiency gain of the IoT. In addition, IoT systems use a wide variety of devices with different features which make the connectivity and coordination process very difficult. Therefore, adopting AI should consider these different components.

3. ***Security and privacy:*** One of the most difficult issues that face most of the new technologies is security and privacy. As IoT systems use sensors that are installed in our surrounding environment. These sensors collect not only environment data but also our habits, financial records, and other sensitive information. Therefore, providing a secure IoT system is a compulsory task to continue its successful deployments in our environment [24]. The IoT is intrinsically vulnerable to most of the wireless common attacks because most IoT devices are connected through wireless networks that are hard to protect against different attacks such as man-in-the-middle attack and other attacks [25]. So, with AI, how security and privacy issues can be reduced?

4. ***Standardization***: There many issues related to IoT standardization such as interoperability, radio access level, semantic interoperability, and security and privacy. The open standards of IoT such as security standards, communication standards, and identification standards, might be several key enablers for the expansion of the IoT technologies [31]. With the lack of appropriate IoT standards, the integration of IoT with AI might face many problems.

5. ***Accuracy and speed***: with the large scale of IoT devices which are in billions, there is a huge amount of data generated from these devices. The main goal of the AI is to use its powerful analytical tools to generate the correct meaning or understanding from this data in short time, especially for real-time IoT applications.

6. ***Blockchain***: Current IoT systems are built on centralized server/client model, which requires all devices to be connected and authenticated through the server. This model would not be able to provide the needs to outspread the IoT system in the future. Therefore, moving the IoT system into the decentralized path may be the right decision. One of the popular decentralization platforms is blockchain [32]. A blockchain is a distributed database of records that contains all transactions that have been executed and shared among participating parties in the network [32]. Integrating IoT with blockchain and AI will have many benefits. For instance, the blockchain will have the ability to handle processing of billions of transactions between IoT devices, which will significantly reduce the costs associated with installing and maintaining large centralized data centres and will distribute computation and storage needs across the billions of devices that form IoT networks. Adopting blockchain with IoT and AI need more research.

7. ***Legal Aspects:*** The IoT system has many integrated services provided by multiple partners, collaborative ventures, and new business models will give rise to legal challenges and legal relationships will need to be addressed between the parties as will liability, IP, privacy, security, insurance and other regulatory issues [33].

8. ***Artificial Stupidity***: Although the huge capabilities that AI can provide in different aspects, it requires training to understand and make a decision [27]. With the lack of appropriate and correct data, AI cannot provide expected benefits to IoT systems.

IX. CONCLUSION

IoT is creating a technological revolution that represents the future of computing and communication. With the IoT, billions of devices can connect and communicate together to share their data. With the rapid increase in the adoption of IoT objects, a huge amount of data is being created, and traditional analytic approaches will not be able to keep up with IoT systems. With the integration of IoT with AI, this problem can be addressed. AI provides new solutions by centralized or

distributed intelligence to analyse and extract meaningful information and provide decision support tools. Using the analytic power of AI with the huge amount of IoT data will release the full benefits of IoT data, which in turn will lead to a variety of benefits for both IoT users and companies. In this paper, we presented an overview of the integration of IoT with AI. It started by discussing essential features of IoT systems with its layered architecture. This is followed by a discussion of the benefits of the integration process with highlighting IoT applications that will benefit from AI. Implementation challenges of IoT with AI are also discussed.

REFERENCES

[1] H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, "Validation of an Adaptive Risk-based Access Control Model for the Internet of Things," I.J. Comput. Netw. Inf. Secur., no. 1 pp. 26–35, 2018.

[2] K. Ashton, "That 'Internet of Things' Thing," RFiD J., p. 4986, 2009.

[3] M. I. Hussain, "Internet of Things: challenges and research opportunities," CSI Trans. ICT, vol. 5, no. 1, pp. 87–95, 2017.

[4] D. Gil, A. Ferrández, H. Mora-Mora, and J. Peral, "Internet of things: A review of surveys based on context aware intelligent services," Sensors (Switzerland), vol. 16, no. 7, pp. 1–23, 2016.

[5] A. Pannu and M. T. Student, "Artificial Intelligence and its Application in Different Areas," nternational J. Eng. Innov. Technol., vol. 4, no. 10, pp. 79–84, 2008.

[6] B. Ragothaman, S. Prabha, E. Jose, and B. Sarojini, "A Survey on Big Data and Internet of Things," in 2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems, 2016, pp. 174–179.

[7] C. M. Chung, C. C. Chen, W. P. Shih, T. E. Lin, R. J. Yeh, and I. Wang, "Automated machine learning for Internet of Things," in 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), 2017, pp. 295–296.

[8] A. Poniszewska-Maranda and D. Kaczmarek, "Selected methods of artificial intelligence for Internet of Things conception," in Federated Conference on Computer Science and Information Systems, 2015, vol. 5, pp. 1343–1348.

[9] Y. Huang and G. Li, "A Semantic Analysis for Internet of Things," in 2010 International Conference on Intelligent Computation Technology and Automation, 2010, no. 2, pp. 336–339.

[10] H. F. Atlam, M. O. Alassafi, A. Alenezi, R. J. Walters, and G. B. Wills, "XACML for Building Access Control Policies in Internet of Things," in in Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018), 2018, pp. 253–260.

[11] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," in Proceedings - 10th International Conference on Frontiers of Information Technology, 2012, pp. 257–260.

[12] R. Shanbhag and R. Shankarmani, "Architecture for Internet of Things to minimize human intervention," in 2015 International Conference on Advances in Computing, Communications and Informatics, 2015, pp. 2348–2353.

[13] G. Joshi and S. Kim, "Survey, Nomenclature and Comparison of Reader Anti-Collision Protocols in RFID," IETE Tech. Rev., vol. 25, no. 5, p. 285, 2013.

[14] ITU, "Overview of the Internet of things," Ser. Y Glob. Inf. infrastructure, internet Protoc. Asp. next-generation networks - Fram. Funct. Archit. Model., p. 22-37, 2012.

[15] H. F. Atlam, R. J. Walters, and G. B. Wills, "Fog Computing and the Internet of Things: A Review," Big Data Cogn. Comput., vol. 2, no. 10, pp. 1–18, 2018.

[16] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," IEEE Internet Things J., pp. 1125–1142, 2017.

[17] S. Shifeng Fang et al., "An Integrated System for Regional Environmental Monitoring and Management Based on Internet of Things," IEEE Trans. Ind. Informatics, vol. 10, no. 2, pp. 1596–1605, 2014.

[18] M. Adda, J. Abdelaziz, H. Mcheick, and R. Saad, "Toward an Access Control Model for IOTCollab," in The 6th International Conference on Ambient Systems, Networks and Technologies, 2015, vol. 52, pp. 428–435.

[19] P. P. Ray, "A survey on Internet of Things architectures," J. King Saud Univ. - Comput. Inf. Sci., pp. 1–29, 2016.

[20] M. S. A. Carlo, "An Overview of Privacy and Security Issues in the Internet of Things," McKinsey Q., vol. 2, p. 6-13, 2013.

[21] D. Chen, G. Chang, L. Jin, X. Ren, and F. Li, "A Novel Secure Architecture for the Internet of Things," in 2011 Fifth International Conference on Genetic and Evolutionary Computing, 2011, pp. 311–314.

[22] K. K. Patel and S. M. Patel, "Internet of Things-IOT : Definition , Characteristics , Architecture , Enabling Technologies , Application & Future Challenges," Int. J. Eng. Sci. Comput., vol. 6, no. 5, pp. 6122–6131, 2016.

[23] R. Reddy and M. Minsky, "The challenge of Artificial Intelligence," Computer (Long. Beach. Calif)., vol. 29, pp. 86–98, 1996.

[24] H. F. Atlam, A. Alenezi, R. J. Walters, and G. B. Wills, "An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things," in Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017), 2017, pp. 254–260.

[25] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and J. Daniel, "Developing an adaptive Risk-based access control model for the Internet of Things," in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, no. June, pp. 655–661.

[26] IDC, "Amount of Data Created Annually to Reach 180 Zettabytes in 2025." [Online]. Available: www.idc.com. [Accessed: 20-Jan-2018].

[27] A. Banafa, "Why IoT Needs AI," 2017. [Online]. Available: https://www.bbvaopenmind.com/en/why-iot-needs-ai/. [Accessed: 20-Jan-2018].

[28] Raman Chitkara, A. Rao, and D. Yaung, "Leveraging the upcoming disruptions from AI and IoT," PWC report, 2017.

[29] H. F. Atlam, A. Alenezi, A. Alharthi, R. Walters, and G. Wills, "Integration of cloud computing with internet of things: challenges and open issues," in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, no. June, pp. 670–675.

[30] K. Xu, Y. Qu, and K. Yang, "A tutorial on the internet of things: From a heterogeneous network integration perspective," IEEE Netw., vol. 30, no. 2, pp. 102–108, 2016.

[31] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," Inf. Syst. Front., vol. 17, no. 2, pp. 243–259, 2015.

[32] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Blockchain with Internet of Things: Benefits, Challenges, and Future Directions," Int. J. Intell. Syst. Appl., p. in press.

[33] N. Kumar, N. Kharkwal, R. Kohli, and S. Choudhary, "Ethical aspects and future of artificial intelligence," in 2016 1st International Conference on Innovation and Challenges in Cyber Security, ICICCS 2016, 2016, pp. 111–114.