Smart Water Sprinkler Based on IoT

Use of Water Sprinkler in Dust Management

Nabin Oli
Bachelor of Science with Honours Computer and Data Science, Sunway College Kathmandu
Birmingham City University (BCU)
Kathmandu, Nepal
Nabin.Oli@mail.bcu.ac.uk

Abstract **—This research article offers a thorough examination of the design and use of intelligent water sprinklers for the control and management of dust particles, especially PM2.5 (Particulate Material 2.5). Finding efficient ways to reduce dust particles present in air is essential given the rising concern over air pollution and its harmful impact on human health. With the use of IoT technology and sophisticated sensing capabilities, the suggested smart water sprinklers can identify peak time interval and activate at right time and target regions with a high concentration of dust. The sprinklers effectively settle down the dust particles by spewing water in minute fragments, resulting in cleaner, healthier air(without dust particles). The results emphasize the system's potential to help improve air quality and show how well its prototype works. The study ends with suggestions for future developments and the use of intelligent water sprinklers for dust control.**

Keywords—Internet of things, Smart Water sprinkler for dust management, Dust Management system

The health of people and the welfare of communities are significantly at danger from air pollution, a major environmental problem on a worldwide scale. The capital city of Nepal, Kathmandu, which has experienced rising air pollution levels, and is one of the areas battling this problem. Kathmandu has the terrible title of being the most air-polluted city in the world and also having PM2.5 concentration in Kathmandu is generally 5.8 times the WHO annual air quality guideline value. It is now more important than ever to solve this pressing problem, which calls for creative and practical solutions to enhance the city's air quality and guarantee the welfare of its residents.

I. LITERATURE REVIEW

The term "Internet of Things" (IoT) describes a network of physically connected devices, each of which has engaged processing, sensor, and actuator capabilities. Through the Internet, which acts as their common communication platform, these items may cooperate and share information with one another. In this situation, the Internet acts as a network to connect people to a wealth of knowledge (Hussein, 2019). The field of the Internet of Things (IoT) is one that is fast developing and has the potential to change several sectors as well as society at large. Over 11 billion IoT devices were in operation as of 2019, and by 2030, that figure is projected to increase to 30 billion (Vailshery, 2022). In this part, we'll give an overview of current IoT developments, forecast, and assess future trends, and talk about basic security.

A. Current IoT trends:

In order to establish a seamless and interconnected ecosystem of devices, systems, and services, the current trend in IoT is toward the integration of multiple technologies and protocols. The convergence of IoT with 5G networks, which allows for ultra-fast data transfer, low latency, and widespread device connectivity, is one of the important advances in this (Liu et al., 2020). With this connection, new IoT use cases and applications, such automated vehicles, smart cities, and industrial automation, may become possible. The advent of digital twins, which are virtual duplicates of real-world systems or objects that allow for simulation, prediction, and behavior optimization, is another trend (Li et al., 2021).

B. Future trends

New trends and ideas are being sparked by the IoT technology's explosive expansion in a number of industries. For instance, edge computing, which places data processing and analysis closer to IoT devices at the network's edge, has become a prominent trend in the IoT (Fernández-Caramés & Fraga-Lamas, 2018). Future IoT developments are anticipated to have a substantial influence on several businesses as well as society at large. For instance: Blockchain integration in IoT is anticipated to increase supply chain management's transparency and security, lowering the danger of fake products and enhancing traceability (Yli-Huumo et al., 2016). Access to healthcare services is anticipated to increase with the adoption of IoT, especially in rural and underserved regions. This could result in better health outcomes and lower medical expenses (Halamka and Tripathi, 2020). New trends and ideas are being sparked by the IoT technology's explosive expansion in a number of industries. For instance, edge computing, which places data processing and analysis closer to IoT devices at the network's edge, has become a prominent trend in the IoT (Fernández-Caramés & Fraga-Lamas, 2018). By limiting the transmission of sensitive data over the network, this strategy decreases latency, increases scalability, and strengthens security.

C. Innovative features in modern computing

IoT Modern computer innovation has completely transformed how we engage with technology and has sparked the creation of several cutting-edge features that improve functionality, efficacy, and user experience. The incorporation of artificial intelligence (AI) and machine learning (ML) algorithms into computing systems is a noteworthy advance. AI-powered technologies improve activities like data analysis, pattern recognition, and natural language processing by allowing computers to learn, adapt, and make wise judgments (Russell & Norvig, 2020). The introduction of edge computing, which allows data processing and storage at the network's edge, closer to the source of data production, is another noteworthy advance (Satyanarayanan et al., 2019). This method minimizes data transfer to centralized cloud servers, which decreases latency, improves real-time responsiveness, and handles privacy issues. In addition, quantum computing has become a promising new field that uses the ideas of quantum mechanics to carry out intricate calculations at a scale never before possible (Preskill, 2018). Cryptography, optimization, and simulation are just a few of the industries that quantum computing has the potential to change. These cutting-edge components of contemporary computing have created new opportunities and set the path for developments in a number of fields.

D. SECURITY

In order to protect user security and privacy, new security issues brought on by the proliferation of IoT devices must be resolved. This section will give an overview of IoT security concerns, analyze various methods and solutions, and emphasize the drawbacks and shortcomings of existing security measures. IoT has received a lot of interest recently from both the business world and academia because of its potential to completely change how we interact with technology and the outside world. Despite the IoT's potential advantages, there are still many obstacles to overcome and issues that need to be resolved in the areas of security, privacy, interoperability, and sustainability (Al-Fuqaha et al., 2015). To create efficient strategies for its implementation and management, it is crucial to comprehend the current status of IoT and its evolution. Given the hazards connected with unauthorized access, data breaches, and malicious attacks, security and cybersecurity are essential factors to consider for IoT systems (Alaba et al., 2017). Securing these systems becomes more difficult as there are more connected devices and IoT networks become more complicated. Authentication and access control, data confidentiality, integrity, and availability, as well as secure communication protocols, are some of the major security concerns in IoT (Jing et al., 2019). Additionally, it is challenging to build standardized security measures due to the heterogeneity of IoT devices and protocols, and the usage of conventional security solutions is constrained by the resource limitations of IoT devices. As a result, new security protocols and solutions that are tailored specifically for IoT systems are required (Al-Fuqaha et al., 2015).

II. TECHNICAL DEVELOPMENT

The automated IoT-based smart water sprinkler was designed and developed for the purpose of dust management. First things first, Extensive research on the components and technologies needed to create an efficient and effective solution for reducing air pollution was done. As the basic water sprinklers components were found. The water sprinkler utilizes a ultrasonic sensor for detecting the human presence near the Smart-Water sprinkler for ensuring no-one gets wet and temperature sensor and moisture sensor for reporting environmental conditions for making intelligent decisions. It includes ultrasonic sensors and IoT command processing unit for detecting human presence and getting readings of dust particles concentration respectively, allowing it to automatically activate when dust levels reach a certain threshold and deactivate when people are nearby.

A. *Purposed system*

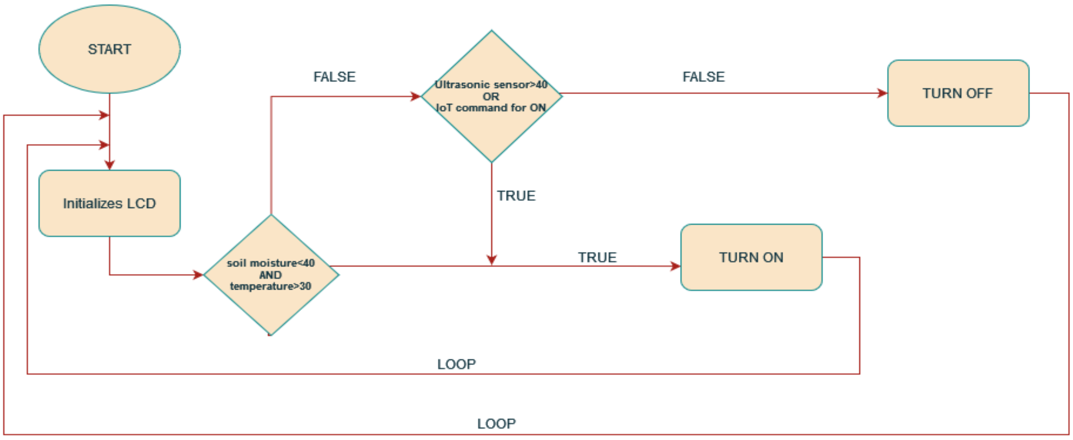


Fig. 1. Smart Water Sprinkler for dust management flowchart

This smart-water sprinkler prototype's performance has been simulated and tested in virtual software in various settings to evaluate its effectiveness in reducing air pollution and water usage. The tests were conducted in TinkerCad settings with varying levels of soil moisture reading, temperature condition and ultrasonic sensor detection for varying length. The sprinkler was activated for a period of time and the movement of DC motor which was used considering water sprinkler movement. The results of the testing showed that the automated IoT-based water sprinkler has high potential in reducing air pollution and settling dust particles.

B. *Methodology for System Design*

TABLE. I TRUTH TABLE OF SYSTEM

CASES	***Moisture sensor***	***Temperature sensor***	***Ultrasonic sensor***	***User command (Wi-Fi Module)***	***Water Sprinkler***
	A	***B***	***C***	***D***	***OUTPUT***
1	0	0	0	0	0
2	0	0	0	1	1
3	0	0	1	0	1
4	0	0	1	1	1
5	0	1	0	0	0
6	0	1	0	1	1
7	0	1	1	0	1
8	0	1	1	1	1
9	1	0	0	0	0
10	1	0	0	1	1
11	1	0	1	0	1
12	1	0	1	1	1
13	1	1	0	0	1
14	1	1	0	1	1
15	1	1	1	0	1
16	1	1	1	1	1

The table I presents a truth table for a smart-water sprinkler system based on logic. The system consists of four input variables: Moisture sensor, Temperature sensor, Ultrasonic sensor, and IoT connection. The output variable is labeled "Output." The table showcases the combinations of inputs and their corresponding output values. Each row represents a unique combination of input values, ranging from 0 to 1. The Moisture sensor, Temperature sensor, and Ultrasonic sensor columns indicate whether each respective sensor is activated (1) or not activated (0). The IoT connection column signifies the presence (1) or absence (0) of an IoT connection. The last column, labeled “Output” presents the resulting output value for each combination of inputs. The output is either 0 or 1, indicating a binary response based on the given inputs. The truth table provides a comprehensive overview of the system’s behavior and helps analyze the relationship between the inputs and the resulting output. Researchers can utilize this table to study and understand the logic and functioning of the system, enabling further analysis, comparisons, or decision-making based on the system’s behavior.

The final equation for the system is:

Equation=(A x B) + (C + D)

In this equation, (A x B) represents the logical AND operation between the temperature and moisture sensors, ensuring both sensors indicate environmental conditions. The result of this operation (AND operation) and (C + D) is combined with OR operation, where C represents the output of the ultrasonic sensor and D represents the input received from the IoT control. This logical OR operation allows the sprinkler to activate when either the temperature and moisture sensors are satisfied, or the ultrasonic sensor detects an obstacle or the IoT control sends a command. By utilizing this final equation, the water sprinkler system can make intelligent decisions based on multiple inputs and control signals, resulting in efficient, flexible and intelligent decisions.

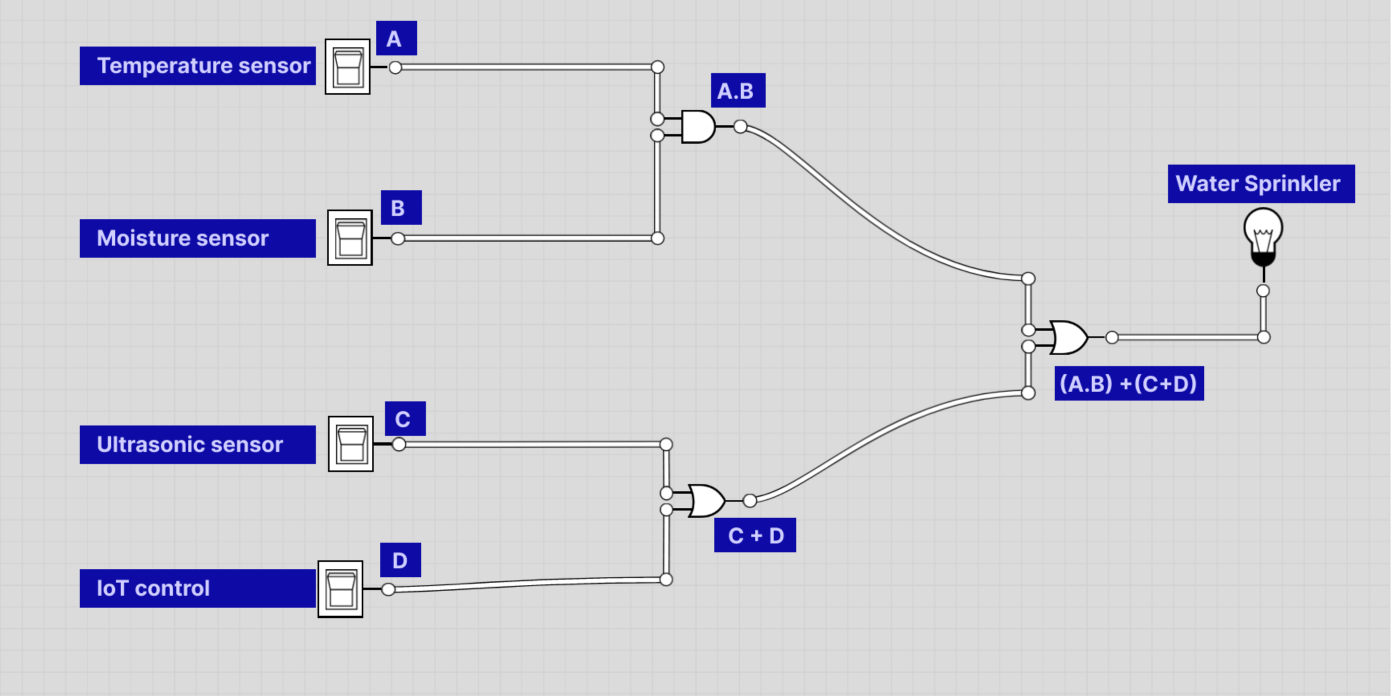


Fig. 2. Smart Water sprinkler for dust management logic circuit diagram

III. HARDWARE REQUIREMENTS

The components used in the Tinkercad platform are listed in the table. Each component has a name, which is connected to a quantity utilized in the setup. The system’s primary control board is the Arduino Uno R3 microcontroller board (U1). It offers the processing power and interfaces required for communication with other parts.

1. U2: LCD 16x2: The 16x2 LCD display is used for visual output, enabling the system to provide text and symbols to users as a means of informing them of information and providing feedback.

2. Rpot1: 250 k Potentiometer: This potentiometer is used in the circuit to regulate variables like voltage or signal levels in the system.

3. U3: Temperature Sensor [TMP36]: The TMP36 variant of this temperature sensor allows for the detection of ambient temperature. It generates analog output according to temperature.

4. DIST2: Ultrasonic Distance Sensor: Ultrasonic waves are employed by the ultrasonic distance sensor to detect distances. It produces sound waves and determines how long it takes for the waves to return from an object to compute distance.

5. M2: DC Motor: The system uses a DC motor for mechanical movement or control. It causes mechanical motion by converting electrical energy.

6. The SEN2 Soil Moisture Sensor is used to find and gauge the soil’s moisture content. It facilitates automated irrigation systems or other soil moisture management applications and aids in the monitoring of soil conditions.

7. Wifi Module (ESP8266): The ESP8266 Wi-Fi module enables wireless connectivity for electronic projects, allowing devices to connect to networks and communicate with other devices or online services. Its small size and affordable wireless capabilities make it a popular choice for IoT applications.

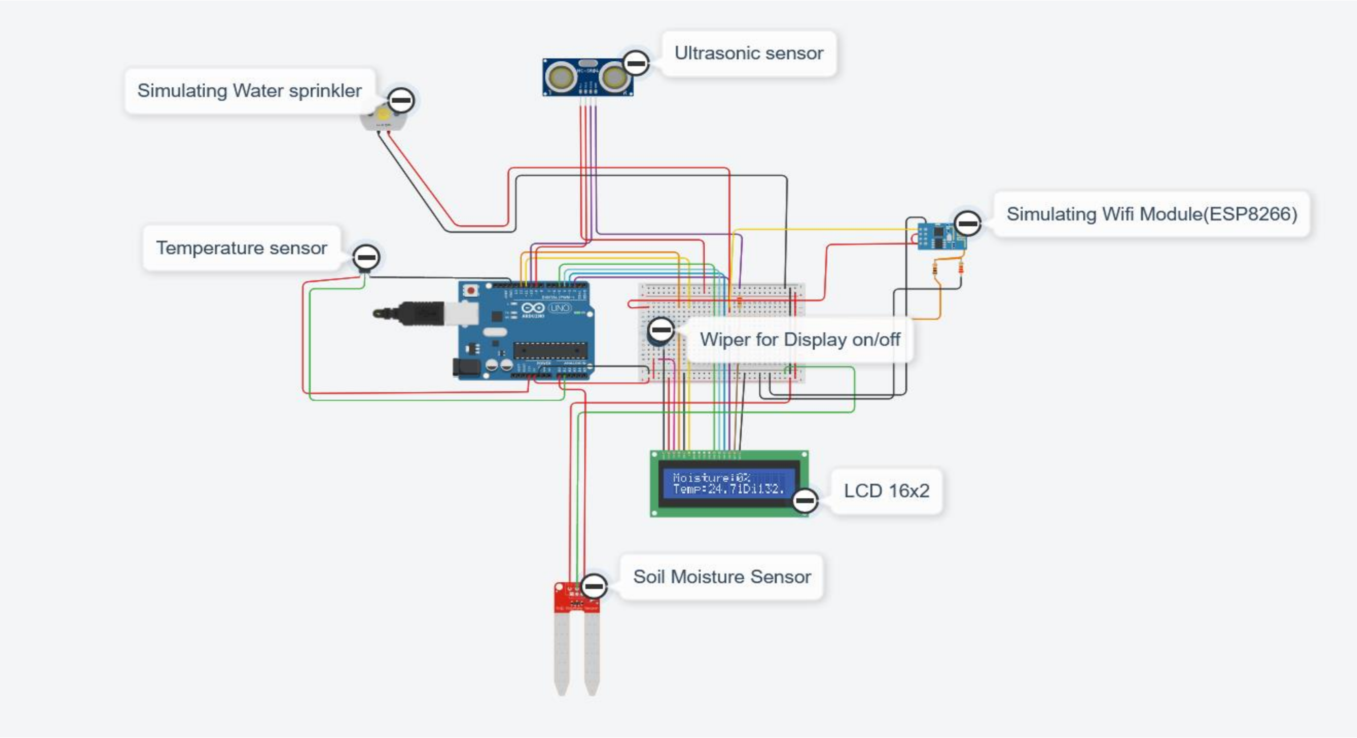
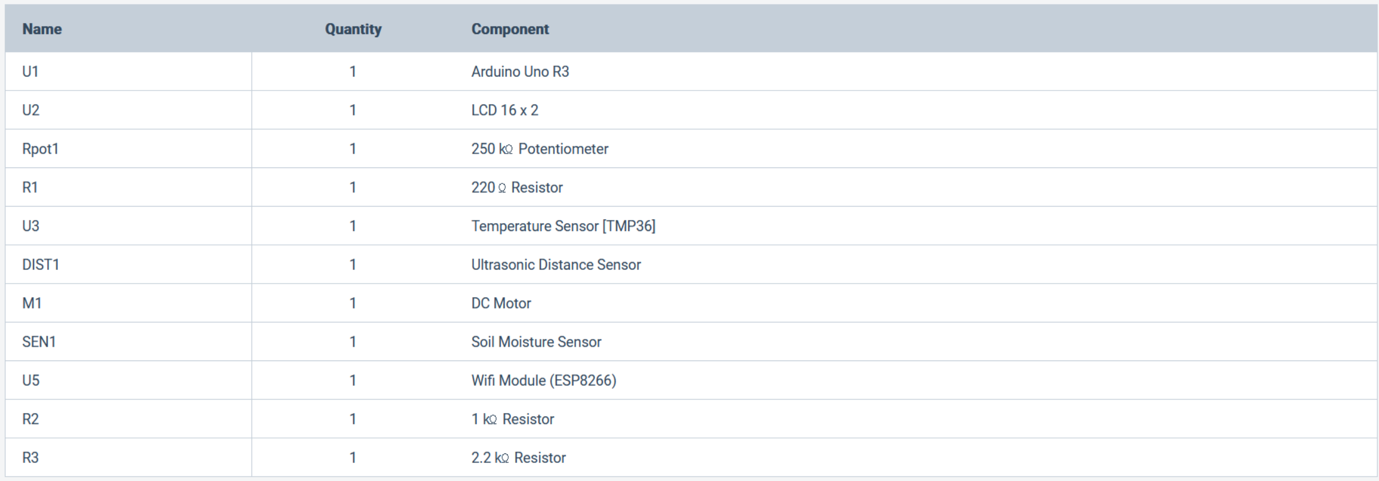


Fig. 3. Smart Water Sprinkler for dust management Tinkercad Design



Name	Quantity	Component
U1	1	Arduino Uno R3
U2	1	LCD 16 x 2
Rpot1	1	250 kΩ Potentiometer
R1	1	220 Ω Resistor
U3	1	Temperature Sensor [TMP36]
DIST1	1	Ultrasonic Distance Sensor
M1	1	DC Motor
SEN1	1	Soil Moisture Sensor
U5	1	Wifi Module (ESP8266)
R2	1	1 kΩ Resistor
R3	1	2.2 kΩ Resistor

Fig. 5. Components List

IV. CONCLUSION AND RECOMMENDATION

In order to efficiently monitor and manage water resources, this research suggests an IoT-based smart water sprinkler system's integration with machine learning algorithm that may enhance the performance of sensors and IoT connectivity. Due to its widespread acceptability and propensity for handling outliers and many variables, the Support Vector Machine (SVM) method is advised to improve usability, efficacy, and precision. In order to enable independent functioning without relying on IoT instructions after two to three years, the system is predicted to collect data from four input devices (three sensors and one IoT control) which will be sufficient for independent functioning. In the initial phase, collection of one week's data will be sufficient for functioning for the next four week with some exceptions(outliers). By putting this autonomous system in place, smart cities' reputation will improve, and operation costs will be reduced. The system's data collection capabilities can also be used in other industries, such as security surveillance, to enable the detection of people using information from ultrasonic sensors. The smart water sprinkler system can independently manage water resources, adjust to changing environmental circumstances, and provide exact watering for each sprinkler by integrating these capabilities. To further improve the efficiency and performance of the system, future study should investigate advanced data analytics techniques. For sustainable urban growth, it is also essential to do in-depth study on autonomous operation and its effect on water management in smart cities. The proposed IoT-based smart water sprinkler system exhibits great promise for effective water management, autonomous operation, and the accomplishment of smart city goals, and the use of the Support Vector Machine algorithm enhances its capabilities and creates opportunities for further research and application in a variety of domains.

V. SECURITY CONSIDERATIONS

The communication between the smart water sprinkler and other hardware or software must be encrypted. This may be done by employing secure communication protocols like Transport Layer Security (TLS) or Secure Shell (SSH), which assist prevent listening in and data manipulation. To manage incoming and outgoing network traffic to and from the smart water sprinkler, a firewall must be installed. The firewall should be set up correctly to only permit trusted and essential communication while obstructing any efforts at illegal access. Strong authentication procedures must be used to prevent unwanted access to the smart sprinkler. This can be done via techniques like digital certificates, multi-factor authentication (e.g., utilizing a mix of passwords and biometrics), or password-based authentication. It's essential for security that the smart water sprinkler's firmware and software are kept current. Patches for discovered vulnerabilities are frequently included in updates, ensuring that the device continues to be secure against them. Secure implementation should be used if the smart water sprinkler permits remote access for monitoring or control purposes. This can be done by creating an encrypted and authorized connection utilizing Virtual Private Network (VPN) connections or secure remote access protocols, including Secure Shell (SSH). The importance of security and recommended techniques for utilizing the smart water sprinkler should be made clear to end users. This can include instructions on how to create secure passwords, keep private information to yourself, identify and report suspicious activity, and routinely update the software on your device. The collection, storage, and transfer of data by the smart water sprinkler should be considered. To protect personally identifiable information (PII), data should be anonymized or encrypted wherever feasible. Additionally, consumers should be openly informed about privacy rules and procedures. The physical equipment itself must be protected, even if this may not directly relate to communication encryption. A device's physical components can be protected by adequate physical security measures, including a tamper-proof shell, which can assist prevent unwanted access.

REFERENCES

Hussein, A.H. (2019) ‘Internet of things (IOT): Research challenges and future applications’, International Journal of Advanced Computer Science and Applications, 10(6). doi:10.14569/ijacsa.2019.0100611.

Vailshery, L.S. (2022) IOT connected devices by technology 2030, Statista. Available at: https://www.statista.com/statistics/1194688/iot-connected-devices-communications-technology/ (Accessed: 05 June 2023).

Liu, Y. et al. (2020) ‘Toward edge intelligence: Multiaccess edge computing for 5G and internet of things’, IEEE Internet of Things Journal, 7(8), pp. 6722–6747. doi:10.1109/jiot.2020.3004500.

Li, Jing et al. (2021) ‘Contract-theoretic pricing for security deposits in sharded blockchain with internet of things (IOT)’, IEEE Internet of Things Journal, 8(12), pp. 10052–10070. doi:10.1109/jiot.2021.3049227.

Fernandez-Carames, T.M. and Fraga-Lamas, P. (2018) ‘A review on the use of blockchain for the internet of things’, IEEE Access, 6, pp. 32979–33001. doi:10.1109/access.2018.2842685.

Yli-Huumo, J. et al. (2016) ‘Where is current research on blockchain technology?—a systematic review’, PLOS ONE, 11(10). doi:10.1371/journal.pone.0163477.

Halamka, J., & Tripathi, M. (2020). The HITECH Era in Retrospect. Journal of the American Medical Informatics Association, 27(6), 918–922. https://doi.org/10.1093/jamia/ocaa130

Russell, S.J., Norvig, P. and Davis, E. (2022) ‘Intelligent Agents’, in Artificial Intelligence: A modern approach. Third. Harlow, England: Pearson Educación, pp. 34–59.

Satyanarayanan, M. (2017) ‘The emergence of Edge Computing’, Computer, 50(1), pp. 30–39. doi:10.1109/mc.2017.9.

Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79.

Al-Fuqaha, A. et al. (2015) ‘Internet of things: A survey on enabling technologies, Protocols, and applications’, IEEE Communications Surveys & Tutorials, 17(4), pp. 2347–2376. doi:10.1109/comst.2015.2444095.

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2019). Security of the Internet of Things: perspectives and challenges. Wireless Networks, 25(8), 4473-4494.

Alaba, F.A. et al. (2017) ‘Internet of things security: A survey’, Journal of Network and Computer Applications, 88, pp. 10–28. doi:10.1016/j.jnca.2017.04.002.

Al-Fuqaha, A., Guizani, M., Mohammadi, M. et al. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17, 2347-2376. https://doi.org/10.1109/COMST.2015.2444095

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2019). Security of the Internet of Things: perspectives and challenges. Wireless Networks, 25(8), 4473-4494.

Alaba, F.A. et al. (2017) ‘Internet of things security: A survey’, Journal of Network and Computer Applications, 88, pp. 10–28. doi:10.1016/j.jnca.2017.04.002.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the Internet of Things. IEEE Access, 6, 32979-33001.

Ling, S. H., Lim, W. K., Hoang, T. M., Heng, S. H., & Perera, C. (2018). Enabling edge intelligence in IoT systems via distributed machine learning. IEEE Communications Magazine, 56(12), 144-151.

Liu, Y. et al. (2020) ‘Toward edge intelligence: Multiaccess edge computing for 5G and internet of things’, IEEE Internet of Things Journal, 7(8), pp. 6722–6747. doi:10.1109/jiot.2020.3004500.