

An Adoption of Internet of Things (IoT) Technologies with Potential Challenges, Ethical Issues, Applications suitable for UAE

Gurpreet Singh¹, Shikha Maheshwari², Rajat Verma³, Ruchi Gaur⁴,
Karan Jain⁴

Department of CSE, Chandigarh University, India¹,

Department of Applied Science, Guru Tegh Bahadur Institute of Technology, Delhi, India²,

School of Architecture, World University of Design, Haryana, India³,

School of Design, World University of Design, Haryana, India⁴

Corresponding author: Gurpreet Singh, Email: aiet.cse.gurpreet@gmail.com

Smart communities are essential to a country's development. Numerous nations have just invested large expenditures in the creation of smart cities to provide environmentally friendly living conditions. The Internet of Things, sometimes known as IoT, is a fast expanding ensemble of networked "things" that have sensors built in to them so they are able to collect and share data online without human interaction. However, just like any other technology, it poses ethical problems that force governments to create rules and regulations to address those worries about this form of technology. The purpose of this research paper is to explore and determine the precise IoT applications that are appropriate for the UAE, analyse any possible challenges that may arise and how they might affect the applications themselves, as well as the privacy and ethical issues that ordinary users may encounter. It also looks at the existing and newly enacted IoT regulations and norms. The goal of this study is to look into how internet of things innovations are being used by contracting companies in Dubai, which is important for promoting the general adoption about the application and utilization of the technologies.

Keywords: Internet of Things, Ethical Issues, Privacy, Intellectual Property, Data Protection, Deploying IoT Applications, Challenges Preventing the Adoption of IoT .

1 Introduction

IoT is a brand-new, emergent technology that reflects the incredible progress of information technology. Although Kevin Ashton, a specialist in digital innovation, first used the word in 1999, it wasn't until 2011 that it took off. It alludes to the power of the Internet as it has been applied to devices other than computers and smartphones. In actuality, Internet usage has been extended to a wide range of additional factors, including processes and the environment. The Internet of Things (IoT) is a comprehensive network that interconnects computers, digital machines, mechanical devices, living beings, and various objects, all equipped with distinctive identifiers, enabling seamless transmission of extensive data through networks without necessitating direct human-to-human involvement [1]. This innovative concept relies on leveraging the Internet to streamline our daily lives and business operations, representing a paradigm shift rather than a singular product or system offered by a company to a broad consumer base.

The Internet of Things (IoT) refers to the ability of all the tools and gadgets we use every day to connect to the Internet and be controlled via a mobile application, a computer, or other Internet-connected control devices depicts in Figure 1. The IoT technology is based on the idea that devices can connect. Computers linked to the Internet were connected

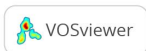
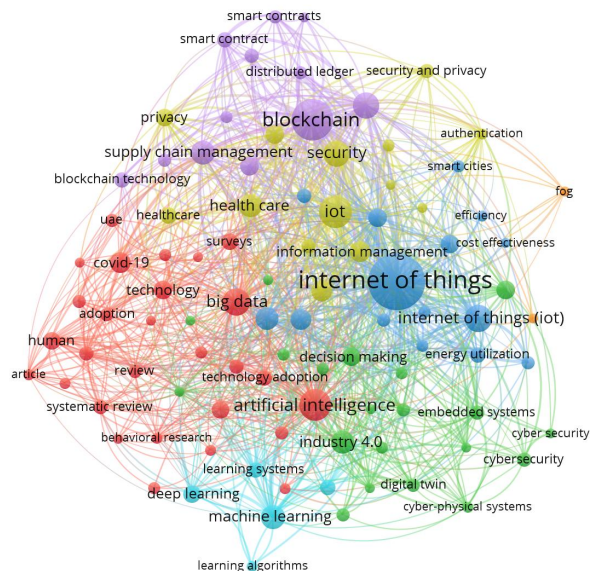


Figure 1: IoT Adoption Driven by Innovative Technology Infrastructure

devices in the 1990s, and there were one billion of these computers. Because cell phones

were also linked with the help of the internet in the 2000s, there were more than two billion connected devices. In 2024, there will be 50 billion connected gadgets, according to predictions [2]. While numerous worldwide firms are competing in a wide range of industries—from agriculture equipment to self-driving cars and manufacture to fitness and health devices—no single corporation has complete market domination. IoT is an ecosystem made up of interconnected hardware and software platforms that use applications to centralize user data. Through related services provided to users-connected devices, this will facilitate the exchange of data with other enterprises and services, fostering the establishment of correlations among diverse data sources. These are physical items that have connectivity, sensors, software, accessories, and other features. The rise of the IoT has produced various kinds of ethical questions about the social, ethical, economic, and social aspects of societies are essential considerations in light of the aforementioned reasons [3]. Choosing how to implement IoT technology in their nation presents challenges and choices for government authorities all over the world. The goal of this study is to raise awareness of these concerns through research because it is crucial to recognize and deal with the aforementioned underlying problems. Such well-documented research offers additional insights, enhancing the necessity and significance of this study.

Additionally, the UAE continues to demonstrate bold adjustments in the IoT while fostering innovation and investment in the rule of law, while numerous countries across the globe are actively engaging in strategic investments to enhance their IoT capabilities[4]. Like most other countries, the UAE is developing a national policy and promoting IoT innovation across all industries given in Figure 2. One of the first Arab nations to consistently gain from technology was the United Arab Emirates. For instance, the Internet of Things has received a lot of attention as a mediator for realizing the Dubai Vision 2021. The government's interest in the IoT and the UAE's high expenditure on it during 2019-2022 are both indicators of how expensive the country is the utilization and funding of IoT are aimed at aiding governments in areas such as security, governance, efficiency, data dissemination, revenue generation, and management[5].

In the UAE, the Telecommunications Regulatory Authority (TRA), analyzing the surge in the IoT industry and the related concerns regarding security and privacy threats compelled the release of the IoT regulatory policy, comprising a set of regulatory procedures and data protection principles. Such material served as the impetus for our investigation of the moral ramifications of IoT usage in relation to the UAE. The country's distinctive position in embracing new technologies and effectively regulating their implementation has driven the need for the IoT regulatory policy[6].

This study is organized as follows: Section 2 of this paper will begin about discussing ethical issues brought up by the IoT, Section 3 will enlist some of the challenges faced

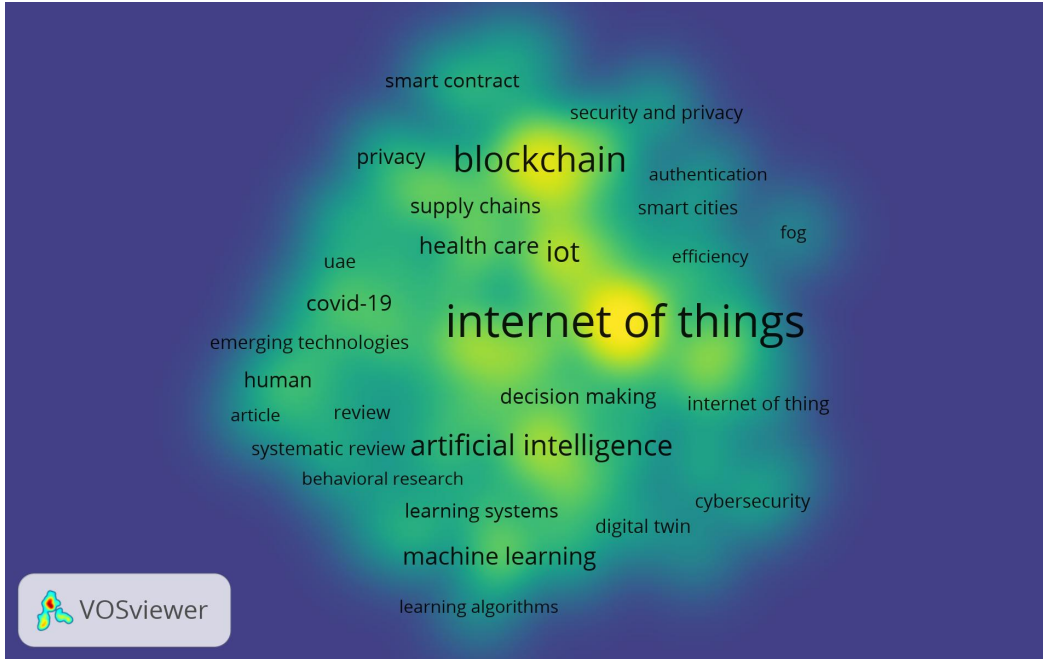


Figure 2: Important aspects of the development of IoT

while the country-wide adoption of IoT, Section 4 will discuss some applications of the IoT underway for development and growth of the nation, and the study will be brought to an end with a conclusion in Section 5.

2 Ethical Issues Caused of IoT Technology

The Internet of Things offers various benefits that will improve human lives and solve significant issues. These include improved customer service, higher-quality products and services, quicker decision-making, better personal life management, more control over time, and safety at facilities are among the many of these. However, multiple shortcomings need to be addressed. It is undeniable that the IoT has made it possible to misuse and abuse it, which leads to ethical and moral concerns that people are likely to face at work. These dilemmas include the need to understand the ethical danger presented by new technology and the difficulty of developing business ethics standards that address IoT concerns[7]. In the absence of system firewalls, hackers exploit methods to lure internet users into providing access to their data as global interconnectivity grows. Consequently, damaged systems and compromised security elevate data protection expenses for businesses or organizations, as data breaches and leaks affecting specific individuals or enterprises can have severe financial and reputational consequences. For instance, the

impact of online client spending following a data breach. Pressure to alter the legal system in order to tighten regulation and lower technological requirements has increased as a result of the IoT. The need to adjust the legal environment grows as the IoT ecosystem becomes more complex[8]. The following guidelines for creating a corporate ethics policy statement to direct people and promote ethical decision making:

2.1 Rights and Obligations Relating to Information

In the past, there has been a significant increase in the number of networked and linked devices. The IoT and connected gadgets clearly have a darker side despite these opportunities. To protect the data derived from IoT systems, similar to other Internet-based systems, they must properly address cyber security and privacy risks. It is impossible to understate how critical the risks relating to security are posed by the explosion of IoT devices in an unsecured environment are. The risk of network devices being readily compromised in terms of security. Sensors that frequently lack adequate security will be easy targets for hackers and may therefore cause issues. Customers genuinely fear these connected devices as they believe that, due to their interconnected nature, their data and privacy might be compromised [9].

In the IoT, the gadgets we use every day—smartphones, smart watches, televisions, refrigerators, heaters, surveillance cameras, smart doors, collect information that enables them to understand our behaviors and our faces, or, more accurately. Such information shows the genuine desires we express when using our products. This will pave the way for us to transition into aggressive consumer cultures where adverts will be presented on devices based on our authentic preferences, rather than relying on website visits and social media interactions.

But it is undeniable that in the IoT and Internet of Everything era, network-connected devices such as computers, smartphones, smart homes, smart home appliances, wearable technology such as glasses, and many more are susceptible to piracy.

These IoT gadgets gather a huge amount of information about us along with all the aspects of our daily life without us being aware that this data will eventually be converted into information and retained on the service providers' servers. These details can be used to improve user experience and offer suggestions. Alternatively, hackers might gain access to that data and release it [10].

In addition to the invasion of privacy, it is important to remember that most of these connected gadgets over the internet available on the market today do not meet specified criteria for electronic protection, making them open to piracy and penetration. As a result, we find it challenging to regulate data possession and protection through legislation, as it may expose systems and services to potential harm and unauthorized commands, leading to significant financial costs or jeopardizing users' safety.

2.2 Intellectual Property Rights and Obligations

Take use of various intellectual property (IP) safeguards, including trademark, patent, copyright, and design protection. Although software are not covered by patents. Although software is not covered by patents It is present in nations like the USA and Japan as well as in European nations. If the software used in the IoT is new, it can provide specific technical results that are protected by patents. Similarly to this, IoT applications are patentable if they offer new services to linked devices. The visual design of IoT devices can also be protected since customers favored one product over another, protecting the functioning of IoT devices through copyright and patent mechanisms poses another significant consideration[11]. Another significant matter that is subject to trademark law protection is the IoT's brand name. Numerous businesses worldwide are spending a significant amount of money due to the IoT's expanding popularity of the money in the creation of their line of Internet of Things (IoT) products and software. Additionally, this has significantly increased the number of patent applications. However, development has been hampered by the standardization and interoperability required for the devices to be able to communicate with one another The problem is that using the patented standard technology will violate the patent of the first user. Additionally, a dispute over who owns the data could arise if two or more devices with various copyrights or patents were combined with patented or copyrighted software that permits the right to gather data.

The issues surrounding data are supported by ownership of personal data, "It also holds substantial implications for the future of data-driven commerce and the "digital" economy". In the IoT age, having a strong patent may be profitable [12], but the IoT also creates a problem with patent trolls, making it necessary to assert such inventions as conventionally necessary patents. The IoT also raises the issue of where to find the data that IoT-integrated devices have acquired. When two connected devices from two different companies gather information about the user of the devices, this causes disputes. The IoT also brings up the issue of shoddy patents, which are conflicting. with each other. The difficulty of protecting IP in the IoT may lead to more allegations of patent infringement [13]. However, the IoT introduces a factor that will make future accusations about infringement of intellectual property rights more difficult. For instance, there will be numerous machines in addition to devices in the manufacturing industry from different manufacturers that will need to communicate with one another to do specific duties. It's possible that the results will coincide with patents. If roles between industries aren't clearly defined, then both products and solutions will compete with one another.

2.3 Control and Accountability

This dimension alludes to the system of responsibility that establishes who is in charge of the Internet of Things. judgment in relation to the liability question. This moral aspect only applies to liability issues involving computers. This problem relates to who is

accountable for software failures and who bears responsibility for them. It is evident that in cases of machine malfunction leading to damage or injury, the responsibility would naturally fall on the software producer and the operator [14]. However, if the IoT device is perceived as a book, holding the author's publisher accountable for any failures may pose challenges. What form of liability should apply if the software is perceived as a service, creating a scenario comparable to that of a telephone network? The idea of responsibility is ethical Who is responsible, Who is responsible who is liable, who is at fault, and the expectation of account-giving are terms used to describe governance. The topic of accountability, as it applies to the governmental sector, commercial corporations, non-profit organizations, and individual settings, is crucial to the conversation. In the context of leadership roles, accountability encompasses the acknowledgment and acceptance of responsibility for policies, decisions, actions, administration, implementation, and governance, commensurate with the scope of the employment position. It also entails the obligation to report, clearly identifying the person or entity responsible for the outcomes and its consequences [15].

2.4 System Quality

When creating information technology applications, this moral dimension addresses the criteria for evaluating the effectiveness of a system and data that urge that individual liberties and societal security be upheld. This idea could also be used to describe system failures and the quality of the data. The terms "system quality" "acceptable" and "technologically feasible" can also be used interchangeably. Simply said, the IoT will operate efficiently with great system quality. In simple terms, a flawless software is crucial for establishing a high-quality, risk-free system, especially for businesses. Subpar system performance often arises from three primary factors: software bugs, hardware or facility failure, and poor input data quality. A strong quality management system is essential for businesses to ensure that their services are of the highest caliber and that goods can satisfy consumer demands. With an amazing quality management system, businesses may improve their goods and services while still adhering to rules that fulfill standards. The development of the IoT improves businesses' efforts to use data more effectively for bettering their operations. Additionally, there is a change in how the organization maintains and develops quality from just one department, but that was in the past because today, a better-quality system benefits the entire business. In accordance with corporate standards, there is no evidence of a quality system throughout the entire company process[16]. Businesses must continue to make improvements in service management.

2.5 Quality of Life

The Internet of Things, or IoT, as it has been called, is a collection of our environment's linked objects. developing applications and services. Such a setting greatly eases our

lives and helps to put the idea of quality of life into practice. It facilitates residents' enjoyment of a way of life. The Internet of Things system, for instance, can make daily tasks easier for the elderly and give them access to specialized services to enhance their life's quality. The idea of being "smart" encourages you to make use of having an Internet connection. For instance, a smart city promises to increase city operations' efficiency while also enhancing residents' quality of life [16]. On the other side, it's anticipated that unemployment will increase and that many workers will cease delivering. Because of this evolution, their labor and skills are no longer needed. The re-engineering of projects could lead to employment losses. Many of the jobs that are currently necessary will end, and it will be challenging to find workers for new positions. People who lose their work are no longer able to live the life they choose. It is well known that IoT and AI initiatives were created to simplify life and cut costs, but they disregard the employment of people. Along with the aforementioned changes, people will grow more lazy and dependent on this modern technology to do their chores, which could lead to a variety of health issues, the first of which is obesity and overweight. The Internet of Things may lead to health risks such as computer keyboard-related repetitive stress injury and computer vision syndrome. Lastly, users may experience stress caused by technology brought on by low-level electromagnetic fields, radiation, and screen emissions. The drawbacks don't end there; they might also lead to a greater reliance on the Internet in our daily lives. There are numerous lessons to be learned from psychological issues and social media's effects [17]. Although the UAE continually strives to maintain a high standard of living, embracing cutting-edge technologies like the IoT is not without expense. The UAE does not have any problems with electricity distribution or equity in the IoT. It is inevitable for the nation to adopt IoTs as a result of economic growth and the emergence based on the knowledge of the economy, but doing so comes at a cost in terms of political, social, and ethical concerns. Nevertheless, the nation is capable to maintain the standard of living that it has long enjoyed.

3 Challenges Preventing the Adoption of IoT

The adoption of the Internet of Things (IoT) faced several challenges. However, keep in mind that the IoT landscape is constantly evolving, and some of these challenges may have been addressed or changed by now[18]. Here are some of the common challenges preventing the widespread adoption of IoT:

- **Security Concerns:** Security remains one of the most pressing and formidable challenges that hinder the widespread implementation of the IoT in UAE. Like many other countries UAE, faces multifaceted issues in securing IoT devices and networks against an ever-expanding array of cyber threats and potential data breaches. As IoT devices become increasingly interconnected and pervasive across

various sectors, including healthcare, transportation, and smart cities, they become attractive targets for malicious actors, hackers, and cybercriminals seeking to exploit vulnerabilities in these connected systems. Therefore, comprehensive and robust security measures are imperative to safeguard the privacy, integrity, and reliability of IoT infrastructure and data.

- **Privacy Issues:** With the rapid proliferation of IoT devices, which inherently collect vast amounts of data from users and their surroundings, concerns over data privacy and the potential misuse of personal information have soared to the forefront of IoT adoption challenges in the UAE. The extensive data generated and processed by IoT devices can provide valuable insights into user behavior, preferences, and daily activities. However, this data often falls into the hands of corporations and organizations, raising ethical questions about data ownership, transparency, and consent. Striking a delicate balance between data utility for innovation and protecting individual privacy rights becomes a critical aspect of IoT deployment in the UAE's evolving digital landscape [17].
- **Lack of Standards:** The absence of universally accepted standards in the IoT ecosystem poses a considerable challenge for stakeholders in the United Arab Emirates. The lack of a cohesive and standardized framework can lead to confusion, complexity, and inefficiencies in the deployment, management, and integration of IoT solutions across different sectors. Establishing robust and widely adopted standards is crucial to ensure seamless communication, data exchange, and interoperability among IoT devices and networks. By embracing common standards, the UAE can streamline IoT development and enhance the overall reliability and scalability of IoT applications [18].
- **Cost of Implementation:** One of the key deterrents to embracing IoT technology for many organizations in the UAE is the considerable upfront cost associated with implementing IoT solutions. Deploying IoT systems often involve substantial investments in hardware, software, sensors, and network infrastructure, which may strain the financial resources of SMEs (Small and Medium-sized Enterprises) and startups. Reducing the cost of entry for IoT adoption and exploring cost-sharing initiatives and partnerships between the public and private sectors could alleviate the financial burden and encourage broader IoT implementation across diverse industries [17].
- **Skills Gap:** Achieving successful integration and operation of IoT solutions necessitates a skilled workforce capable of developing, managing, and maintaining these sophisticated systems. However, a significant skills gap may hinder the UAE's progress in realizing the full potential of IoT technology. The rapid pace of technological advancements and the evolving nature of IoT applications demand a work-

force proficient in areas such as data analytics, cybersecurity, software development, and hardware engineering. Investing in training and education programs, fostering collaboration between academia and industry, and attracting skilled professionals to the UAE can help bridge the skills gap and create a sustainable IoT ecosystem [18].

- **Energy Efficiency:** As the IoT ecosystem expands, concerns over energy consumption and environmental impact become increasingly important. IoT devices often require power to function, and ensuring their energy efficiency is crucial to minimizing their carbon footprint and extending battery life. Emphasizing energy-efficient designs and sustainable practices in IoT development can contribute to the UAE's commitment to environmental conservation and responsible technology adoption. By promoting green IoT solutions, the UAE can set an example for other regions and industries seeking to leverage IoT technology while mitigating their ecological footprint.

4 Deploying IoT Applications Underway in UAE

The United Arab Emirates (UAE) has demonstrated a proactive approach in adopting and implementing IoT technologies, deploying large-scale applications across diverse sectors depicted in figure 3. The country's government has displayed a strong dedication to advancing its transformation into a smart and interconnected hub, utilizing cutting-edge IoT solutions to enhance efficiency and connectivity in various domains [19]. Some of these applications are:

- **Smart Cities:** The UAE is actively implementing IoT technologies to build smart cities that enhance urban living and sustainability. In cities like Dubai and Abu Dhabi, IoT plays a crucial role in managing various urban aspects. IoT-enabled smart traffic management systems optimize traffic flow and lessen congestion by using real-time data from cameras and sensors. IoT-enabled smart streetlights vary their brightness in response to ambient light and occupancy, leading to energy savings. Additionally, smart surveillance systems enhance public safety by using IoT-powered cameras with advanced analytics to detect potential security threats [19].
- **Energy Management:** IoT applications are transforming energy management practices in the UAE. Smart grids with IoT sensors enable real-time monitoring and control of energy distribution, ensuring efficient utilization and reducing energy wastage. In buildings, IoT-powered energy management systems regulate lighting, heating, and cooling based on occupancy and environmental conditions, optimizing energy consumption and reducing the carbon footprint. Moreover, IoT-enabled

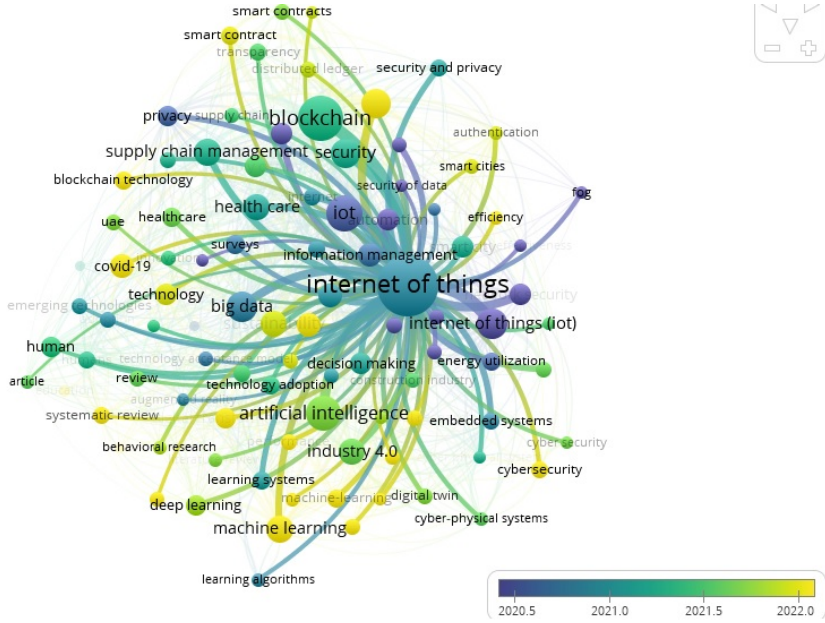


Figure 3: Adoption of the Internet of Things (IoT) in UAE: Large-Scale Applications

smart meters provide consumers with detailed insights into their energy usage, encouraging conservation and sustainable energy practices [20].

- **Transportation and Logistics:** The UAE’s transportation and logistics sectors benefit significantly from IoT implementations. IoT-enabled tracking systems in logistics operations monitor the movement and status of goods, vehicles, and shipping containers. These real-time insights help optimize transportation routes, reduce delivery delays, and enhance supply chain efficiency. In the public transportation domain, IoT applications enable smart bus stops with real-time arrival information and smart ticketing systems for seamless travel experiences [21].
- **Healthcare:** IoT is revolutionizing healthcare in the UAE, enabling advanced remote patient monitoring and personalized healthcare services. Wearable IoT devices collect real-time health data, including vital signs and activity levels, enabling medical professionals to keep an eye on patients from a distance and take prompt action. IoT-powered medical equipment in hospitals streamlines patient care, ensuring timely diagnostics and treatments. Additionally, IoT-based health management platforms empower individuals to take charge of their health by tracking fitness and wellness data [22].
- **Agriculture:** In an effort to enhance agricultural productivity and sustainability,

the UAE is investing in IoT applications for precision farming. IoT sensors and connected devices monitor soil moisture, temperature, and nutrient levels, providing farmers with valuable data for optimizing irrigation and fertilization practices. Smart irrigation systems based on IoT technology help conserve water by delivering precise amounts only when needed. Moreover, IoT-driven agriculture automation enables remotely controlled greenhouses, reducing manual labor and ensuring optimal growing conditions for crops [22].

5 Conclusion

Human beings have been significantly impacted by the speed at which new technology for communication and information is developing. Today, innovation plays a crucial role in everyday life. The purpose of this investigation is to assess and pinpoint various IoT applications that are appropriate for the UAE, as well as to examine possible hazards and their effects on such applications. The study of this article examined a variety of IoT applications, identifying intelligent homes, intelligent towns, and smart health as the three most important ones for the United Arab Emirates. It also examined their mapping. This paper also examined the affordability of these amenities would be in the UAE. Further research on this paper endeavour will concentrate on how different IoT applications can be successfully utilised in the UAE as well as ways they address ethical issues, familiarity with IoT technologies, aspects boosting their adoption, obstacles obstructing their use, alongside the influence of IoT technologies.

References

- [1] Ghandour, A. and Woodford, B.J., 2021. Regulating Internet of Things: The Case of the United Arab Emirates.
- [2] G. Singh and J. Singh, "A Fog Computing based Agriculture-IoT Framework for Detection of Alert Conditions and Effective Crop Protection," 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2023, pp. 537-543, doi: 10.1109/ICSSIT55814.2023.10060995.
- [3] Al-Amleh, K., 2020. A study into the adoption of internet of things–IoT technologies within contractors in Dubai, United Arab Emirates (Doctoral dissertation, The British University in Dubai (BUiD)).
- [4] Awawdeh, M., Bashir, A., Faisal, T., Alhammadi, K., Almansori, M. and Almazrouei, S., 2019, March. Embedded ventilation air conditioning system for protection purposes with IoT control. In 2019 Advances in Science and Engineering Technology International Conferences (ASET) (pp. 1-6). IEEE.
- [5] Younies, H. and Al-Tawil, T.N.E., 2020. Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*, 27(4), pp.1089-1105.
- [6] G. Singh and J. Singh, "A Cost Effective IoT-Assisted Framework Coupled with Fog Computing for Smart Agriculture," 2023 IEEE 8th International Conference for Convergence in Technology (I2CT), Lonavla, India, 2023, pp. 1-8, doi: 10.1109/I2CT57861.2023.10126231.
- [7] Jeyanthi, N.: Internet of Things ((IoT)) interconnection of Threats ((IoT)). Security and Privacy in Internet of Things ((IoT's): Models, Algorithms, and Implementations. Fei Hu (Ed)., CRC Press (2016).
- [8] Chandramma, C., Prakash, P., Nandankar, P., Roopa, H., Kathir, I. and Singh, P., 2023, March. Automation of camel race by controlling DC motor speed using Blynk application through IoT. In AIP Conference Proceedings (Vol. 2690, No. 1). AIP Publishing.
- [9] Hafeez, P.A., Singh, G., Singh, J., Prabha, C., Verma, A.: IoT in Agriculture and Healthcare: Applications and Challenges. In: 3rd International Conference on

- Smart Electronics and Communication (ICOSEC), Trichy, India,,pp. 446-450,(2022)
doi: 10.1109/ICOSEC54921.2022.9952061
- [10] Singh,J., Singh, G., Aggarwal, G.: Inclusion of Aerial Computing in the Internet of Things: Prospects and Applications. In: Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICT), pp. 1664-1669(2022).
- [11] Olushola, O. B. (2019). Factors affecting IoT adoption. *Journal of Computer Engineering*, 21(6), 19-24.
- [12] Olanrewaju, A., Tan, S. Y., & Kwan, L. F. (2017). Roles of communication on performance of the construction sector. *Procedia Engineering*, 196, 763-770. doi:10.1016/j.proeng.2017.08.005.
- [13] G. Singh, S. Pathak, J. Singh and S. Tiwari, "Implication of Mathematics in Data Science Technology Disciplines," 2022 IEEE Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India, 2022, pp. 1-6, doi: 10.1109/IATMSI56455.2022.10119311.
- [14] Oke, A., Aigbavboa, C., & Mabena, S. (2017). Effects of automation on construction industry performance. *Proceedings of the Second International Conference on Mechanics, Materials and Structural Engineering (ICMMSE 2017)*. doi:10.2991/icmmse-17.2017.61
- [15] Razzaq, M.A., Qureshi, M.A.: Security Issues in the Internet of Things (IoT): A Comprehensive Study. *International Journal of Advanced Computer Science and Applications*, 8(6), (2017).
- [16] J. Singh, G. Singh, A. Verma, K. Kaur and Muskan, "IoT Coupled Healthcare Systems: A Bibliometric Analysis," 2022 IEEE Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India, 2022, pp. 1-6, doi: 10.1109/IATMSI56455.2022.10119398.
- [17] Ofori, G. (2016). Challenges facing building construction in developing countries. *Decision Support for Construction Cost Control in Developing Countries*, 28-76. doi:10.4018/978-1-4666-9873-4.ch003
- [18] Mordor Intelligence. (2020). UAE Construction Market - Growth, Trends, and Forecast (2020 - 2025). Retrieved from <https://www.mordorintelligence.com/industry-reports/uae-construction-market>
- [19] Prabowo, S., Abdurohman, M. and Nuha, H.H., 2023. Internet of Things Security and Privacy Policy: Indonesia Landscape. In *Information Systems for Intelligent*

Systems: Proceedings of ISBM 2022 (pp. 201-210). Singapore: Springer Nature Singapore.

- [20] Alharbi, R. and Almagwashi, H., 2019, August. The Privacy requirements for wearable IoT devices in healthcare domain. In 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 18-25). IEEE.
- [21] Hacid, H., Outay, F., Paik, H.Y., Alloum, A., Petrocchi, M., Bouadjenek, M.R., Beheshti, A., Liu, X. and Maaradji, A. eds., 2021. Service-Oriented Computing–ICSOC 2020 Workshops: AIOps, CFTIC, STRAPS, AI-PA, AI-IOTS, and Satellite Events, Dubai, United Arab Emirates, December 14–17, 2020, Proceedings (Vol. 12632). Springer Nature..
- [22] Aljumah, A.I., Nuseir, M.T. and El Refae, G.A., 2022, November. Internet of Things (IoT): A Way to Expedite Production and Service Performance Empirical, Evidence from Textile Industry of United Arab Emirates (UAE). In 2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (pp. 1-8). IEEE.