

# Regulating Internet of Things: The Case of the United Arab Emirates

Ahmad Ghandour<sup>1</sup>, Brendon J. Woodford<sup>2</sup>

<sup>1</sup>College of Business, Al Ain University, Abu Dhabi Campus, Abu Dhabi,

<sup>2</sup>Second Department of Information Science, University of Otago, Dunedin, New Zealand

**Abstract** – The Internet of Things is an important component of the smart technology era. It is the way the world is now moving at an accelerated pace. It has enormous benefits to individuals, groups, companies, and enterprises. Like any other technology, however, it brings ethical challenges requiring governments to develop a legal framework to address those concerns over this technology. This study investigates these challenges in the context of the United Arab Emirates as the government has imposed policies to safeguard the ethical use of the Internet of Things. The study concludes that IoT is a sought-after innovation in the UAE but suffers from deployment without compliance to current regulations and ethics which is becoming mandatory.

**Keywords** – IoT, IoT regulation, moral dimensions, ethics, the UAE

## 1. Introduction

The Internet of Things (IoT) is a new emerging technology in the parlance of the tremendous advancement of Information Technology.

Although the term (IoT) was coined by the expert on digital innovation Keven Ashton in 1999, it only gained momentum in 2011. It refers to the power of

Internet that has been extended beyond the use of computers and other gadgets such as smartphones. The use of the Internet in fact has been expanded to the entire range of other aspects like processes and environment. Specifically, the IoT is a system that aims to interrelate computing devices, digital machines, mechanical apparatuses, animals, people and objects that provide unique identifiers and with limitless capacity voluminous data over a network that does not require any more human-to-human and human-to-computer interaction. It is not a specific product or system that is produced by a company that will be sold to millions of users, rather it is a new concept that depends on the use of the Internet to facilitate the way we live and the way we manage our business [1], [2], [3].

IoT means that all the devices and tools that we use in our daily life have the ability to connect to the Internet and are managed through the mobile application or through the computer or through control devices that are also connected to the Internet. The technology of the IoT depends on the principle that devices communicate with each other. In the nineties the connected devices were computers connected to the Internet and the number of these computers reached one billion connected devices. In the 2000s, the connected devices were in excess of two billion devices because the cell phones were also connected to the internet [4]. The number of connected devices in 2020 was predicted to hit 50 billion [5]. While no single company controls the market, many global players compete in a variety of fields from fitness and health devices to agricultural equipment, infrastructure and smart city building, to the production self-driving cars and drones and more. The IoT is the ecosystem created by connected devices (hardware) and the Internet via platforms (software) that use application (service) to centralize user data. This will enable the exchange of such data with other companies and services and establish correlations between the various data sources through associated services offered to users-connected devices. These are physical objects fitted with accessories, software, sensors and connectivity

---

DOI: 10.18421/TEM103-04

<https://doi.org/10.18421/TEM103-04>

**Corresponding author:** Ahmad Ghandour,  
College of Business, Al Ain University, Abu Dhabi Campus,  
Abu Dhabi, UAE.


**Email:** [ahmad.ghandour@aau.ac.ae](mailto:ahmad.ghandour@aau.ac.ae)

*Received:* 02 May 2021.

*Revised:* 25 June 2021.

*Accepted:* 02 July 2021.

*Published:* 27 August 2021.

 © 2021 Ahmad Ghandour & Brendon J. Woodford; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

The article is published with Open Access at [www.temjournal.com](http://www.temjournal.com)

systems (e.g., radio-frequency identification (RFID) chips) that communicate through a network [6].

For these reasons stated above, the emergence of the IoT has raised a range of ethical issues related to the moral, legal, economic and social aspects of societies. Government officials around the world face challenges and choices regarding how to apply the IoT technology in their country.

Therefore, the rationale behind this study is to draw attention to these issues through research as the need to identify and address the aforementioned underlying issues cannot be overemphasized. Such documented research provides further insights strengthening the need for and the importance of this study.

Furthermore, while many countries around the world are investing strategically in their IoT capabilities, the United Arab Emirates (UAE) continues to show signs of audacious shifts in the rule of law to make innovation and investment in the IoT. Like most nations, the UAE is not only setting up a national strategy but also encouraging investment of the IoT innovation across all sectors. The UAE was one of the first Arab countries to always benefit from technology. For example, great attention has been given to the IoT as a catalyst for achieving the Dubai Vision 2021<sup>1</sup>. The UAE also spends a lot of money on the IoT, evidenced by the government's interest in it, as it spent around 2.4 billion dirhams during 2019<sup>2</sup>. The reason behind applying it and spending on it is to help the state in governance, management, speed, publishing, monetization, and security [7].

In light of the rapid developments in the field of IoT and its applications in the UAE, many experts and policy makers demand the need to set limits through rules governing its work. And to ensure that its use in different sectors does not lead to negative consequences for humans or other systems. At the same time, these rules should not stand as an obstacle to the development and innovations that develop on a daily basis.

Further, in the UAE, the boon of the IoT industry and the related security and privacy risks has pushed the Telecommunications Regulatory Authority (TRA) to issue the IoT regulatory Policy and a set of regulatory procedures as well as setting forth some data protection-related principles.

Such information has motivated our research into the ethical issues around the use of the IoT and how it pertains to the UAE. This is because of the unique position the UAE has in the way it has adopted new

technologies and the means of how it has regulated their use.

This study is structured as follows, in Section II ethical issues raised by the IoT will begin this article followed by Section III discussion, where an analysis of the study will be explored. A conclusion in Section IV will end this research.

## 2. Ethical Issues Raised by the IoT

There are many positives provided by the IoTs that will help facilitate human life and eliminate major problems. These include customer services provision improvements, improve the quality of products and services, expedite decision making, management of personal life, more control over time and protection of facilities, to mention a few. On the other hand, there are negatives that must be addressed. Indeed, the IoT has opened the door to potential misuse and abuse which creates moral and ethical dilemmas that people are likely to face in their workplace [8], [9], [10]. These dilemmas are the need to understand the moral risk of new technology and the difficulty of establishing corporate ethics policies that address the IoT issues.

As the world becomes more connected, hackers find ways to attract Internet users to give them access to their data because there are no system firewalls. Damaged systems and loss of system security lead to the financial burden of companies or organizations on data protection because data breaches and data leaks that allocate individuals and businesses can be expensive and devastating for companies or organizations. For example, the effect of customer online spending after a data breach [11]. Through the use of the IoT, pressure has increased to change the legal environment to tighten regulation and reduce the standards adhered to by technology. As the IoT environment becomes more sophisticated, the pressure to change the legal environment increases [12].

[13] identify five moral dimensions that corporations should use to develop a corporate ethics policy statement to guide individuals and to encourage appropriate decision-making. The policy areas are:

### 2.1. Information Rights and Obligations

The past has seen a massive rise in the number of connected and networked devices. But despite these opportunities, there is undoubtedly a darker side to the IoTs and connected devices. Just like other Internet-based systems, the IoT must deal effectively with cyber security and privacy threats to protect data distilled from the IoT systems. The boom in the IoT devices in an unprotected environment poses critical security challenges that cannot be underestimated.

<sup>1</sup> <https://www.vision2021.ae/en>

<sup>2</sup> <https://www.tahawultech.com/industry/technology/iot-spending-in-mea-to-surpass-8-billion-this-year-idx/>

The vulnerability of network devices' security and the danger of them being easily hacked. Sensors that tend to be improperly equipped with decent security will be vulnerable to hackers and can thus lead to problems. Knowing that, it is also clear that consumers have a real fear of these connected devices which in their view invade their privacy and thus expose it to the risk of penetration [14].

In the world of the IoT, devices around us, smart phones, smart watches, television, refrigerators, heating devices, surveillance, smart doors and cars, all collect data that can recognize our faces, understand our behaviours, rather, know what we want and how we think. Such data reflects our true desire that appear on our devices. This will open the door to transforming into fierce consumer societies, where advertisements will appear to us on devices based on our true desires and not based on our visits to websites and our follow-ups on social media [8].

But what is certain is that in the era of the IoTs and the Internet of everything, network-connected devices are at risk of piracy, from the computer and smartphone, to the smart home and smart home gadgets, to wearable gadgets such as glasses and many more [15].

IoT devices collect a lot of data and every detail in our lives without our awareness that data will transform into information stored on the servers of the service providers. While such data can be used to improve the experience and offer suggestions, it can also be viciously exploited against individuals such as celebrities and political figures. Or in another case, hackers could access that data and leak it [16].

Among the other downsides of this field other than penetrating privacy, it is noteworthy that many of these Internet-connected devices in the market today lack specific standards for electronic protection, so they are vulnerable to piracy and penetration. Because of that reason we find that it is difficult to control (the possession and protection of data regulation) for systems and services to be subjected to specific damage and to issue orders other than the ones we issued, which would incur material costs or endanger users' lives.

The breaches will become more dangerous as it is possible to paralyze a certain community targeted by a particular country, by manipulating electricity meters and issuing orders to close rooms and facilities in its various sector, prevent people from exiting them, permanently halting traffic, leaking video clips from surveillance devices, easily finding targeted people and penetrating stock exchanges, which may result in a major economic, financial or societal setback. [17].

Therefore, consumers are increasingly concerned about security vulnerabilities that may lead to privacy and data breaches and even threaten human

life [18]. These concerns are very legitimate in this networked environment, as with every development we are experiencing in this digital age, the danger of these devices increases and the professionalism of the criminals of the Internet hackers increases.

It is a paramount to provide adequate protection for the software and hardware programs used to network "things" with each other, as well as those who use and receive them. This is because expanding the scope of these activities and their networking will open the door wide for cybercrimes and the cybercriminals who are waiting for this opportunity to pounce to commit multiple cybercrimes, especially Internet crimes. Here, we need modern and sophisticated penal laws to cover the cybercrimes that will emerge due to the spread of the "Internet of Things", and it must be defined to deter criminals as is the case with the EU [19]. Bearing in mind that cybercrime in all its forms is one of the greatest threats to the continuation of the modern technological revolution. But our urgent need for technology in all aspects of our life makes us stand in the way of electronic crime by preparing the necessary laws to combat these crimes and their perpetrators.

The right legal kit will provide the appropriate environment for the continuation of all aspects of the information technology revolution, and reap the benefit from the "Internet of Things" technology that will follow as a natural product and development of the technical revolution that will not stop [19].

Although UAE has no data protection law, the newly regulations of the IoT Policy and Procedures put forward by the TRA may be acted upon as such. Such regulation is aiming at developing safe and secure environment.

Therefore, in the IoT ethics, the aspects of the infringement of privacy rights and system penetration are major concerns, and they remain pertinent for all users in all industry.

## ***2.2. Intellectual Property Rights and Obligations***

Like any other technology, the IoT ecosystems can claim different intellectual property (IP) protection such as copyright, patent, design, and trademark. While software is excluded from the scope of patents in European Countries, it is included in others like the USA and Japan. The software in the IoT is embedded in the connected devices producing specific technical results which can claim patent protection if contribution is innovative. Similarly, IoT applications are patentable if they give the connected devices new services. Beyond the functionality of the IoT devices protected by copyright/patent, the appearance design can also be protected as customer preferred one product over

another. The brand name of the IoT is also another important issue which can be protected under the trademark law [6].

The growing trend of the IoT is making many companies around the world to spend a huge amount of money in the development of their version of IoT devices and applications. This has also led to a tremendous increase in the number of patents filings. However, this has been hampered by the standardization and interoperability required for the devices to be able to communicate with each other. The issue arising is that when the standardized technology patented is used by one it will infringe the patent of the former [20]. Additionally, in the case of patented or copyrighted software that gives the right to collect data, it will create dispute on the ownership of this data if two or more devices with different copyright/patent were connected. The ownership of data is important as the economic model of the IoT is based on the revenue generated from the collected data. "Ownership of personal data underpins the issues revolving around data management and control, such as privacy, trust, and security, and it has also important implications for the future of the 'digital' economy and trade in data" [21]. Possession of a robust patent in the world of the IoT may be lucrative [22] but the IoT raises an issue of patent trolls thus necessitating the need for assertion of such patents as standard essential patents. The IoT also raises an issue of difficulty in ascertainment of the data gathered by the IoT assimilated devices. This brings about disputes in a case whereby two connected devices of twofold distinct companies gather data regarding the consumer of the devices. Another issue raised by the IoT is the one who gets to monetize the gathered data since it's hard to ascertain the owner of the data as companies gather more and more information regarding their activities. The IoT also raises an issue of poor quality of patents, and which are colliding with one another. Safeguarding an IP in the IoT is complicated and may contribute to increased patent violation complaints [9]. Nevertheless, the IoT brings an aspect that will see intellectual property rights have increased difficulty besides contravention complaints in the future. For instance, in the field of manufacturing, there will be a lot of machines besides devices from various manufacturers which will require to converse with one another to finish certain tasks. The outcome of this may be coinciding with patents. In the extreme, the difference amongst industries' roles will be unclear thus both the product and solutions will be rivalling between themselves. Standardized technology is used for the IoT and its interoperability to function on its high and best level to communicate with each other. If these standardized technologies are patented, then it can

adversely impact competition in the market and hinder the performance of the IoT industry all over the world. This will create issues for parties suing patented standardized technology as it will infringe the patent of the past owner. Patent trolls are also on the rise as such patents are being declared as standard essential patents which is then patented to the third parties by fraud. Some software is not protected by patents which cannot protect the source code. This restriction can only be limited to software and not to product, processes and devices in which software is used. It is only possible to protect both software and hardware when software of the IoT is software coupled with hardware combination under computer related inventions [20].

### **2.3. Accountability and Control**

This dimension refers to the accountability structure that governs who is accountable for the IoT decision in case the issue of liability is concerned. Also, this moral dimension is exclusive for computer-related liability problems. This issue is with regards when software fails, and who is to account and responsible for the failure. When failure is part of the machine that causes harm or injury, it would be clear that the software produces, and operator will be held liable. On the other hand, if seen as similar to book, it would be difficult to hold the publisher of an author responsible for its failure. What should be the type of liability if software is seen as service, the situation that is similar to telephone system not being liable for the message transmission [23].

The concept of accountability is an ethics and governance that refers to the question who is answerable, who is to blame, and who is liable and the expectation of account giving. Accountability as an aspect of governance is vital to the discussion which relates to the issue of the public sector, the private corporation, the non-profit and individual contexts. As regards leadership roles, accountability is the assumption and acknowledgment of the responsibility for products, actions, policies, decisions that include governance, administration, and implementation with the limit of the role of employment position and encompassing the report obligation, which explains who will be responsible for the outcome and the result of consequences [24].

In the context of governance, accountability expands beyond the basic definition of being who is to account for one's action. Oftentimes referred to as an account-giving relationship between individuals like for instance, "A" is accountable to "B" when "A" is obliged to inform "B" about the former decisions to justify them and to suffer punishment in the case of eventual conduct. It is therefore

understood that accountability cannot exist without the proper accounting practices and in the absence of accounting means and absence of accountability [25].

In the case of the UAE, the government must have an in-place management control of who will be held accountable for the IoT decision in case of the issue of liability is concerned. When the government fails to have its measures of control, no one among the individuals will be held accountable for their actions. For example, when government does not have management control over the crime of cyberbullying, the government can be blamed when the cyber bullying case is brought to court. Also, it is noticed that the UAE has been implementing with leniency of the cases of cyberbullying since cyber bullying is part of the bigger picture of Internet of Things. Since it is easy to destroy, slander of malign your enemy over the Internet and even just sending an SMS with derogatory content is easier nowadays. Without the proper management control, individuals and groups can easily commit crimes against another individuals, groups or organization and can even extend its harm and destruction to enterprises.

#### 2.4. System Quality

This moral dimension tackles the standards of data and system quality in case we demand to protect individual rights and the society's safety when developing information technology application. Also, this concept may refer to data quality and errors in the system. System quality may refer as well to what system quality is acceptable and what system quality is technologically feasible. Simply, strong system quality will enable smooth functioning of the IoT. In short, it requires flawless software to attain the standards of quality system that is risk free for individuals and groups and most especially for enterprises. There are three principal sources of poor system performance, namely, the hardware or facility failure, software bugs and the poor input data quality which is considered the most common source of failure of software quality among enterprises.

Robust quality management system is critical to business in making sure that the business' services and products can meet customers' needs. With exceptionally good quality system, it helps enterprises comply with regulations that meet the standards while improving their products and services. The creation of the IoT increases the efforts of enterprises in making the best use of data to improve their business operations. Also, within the organization, there is the shift in the maintenance and improving quality from a single department only but that was before, because today, the improvement of quality system improves the entire organization. A quality system is now noticeable in every stage of the

business processes in compliance with business improvement and enterprises need sustain the management of the services that can improve business processes effectively and efficiently especially in the area of the IOT for healthcare [26].

This moral dimension may be effective in combating possible crimes that can be committed in connection with the creation of the IoT such as fraud in the installation of software or any system that can facilitate the Internet of Things. The United Arab Emirates must have an in-place quality system control management so that businesses will continue to have the excellent delivery of their products and services. Quality system is a requirement in the UAE considering that the country is hub to local and foreign investments and in order to lure investors especially in this time of pandemic, the government must have a law to minimize if not to stop completely providers that continue to install poor system quality because it can destroy the image of the UAE government being a very friendly country when it comes to business investments.

#### 2.5. Quality of Life

As it has been described, the IoTs is the group of devices around us that are connected to the Internet creating services and applications. Such environment makes life much easier for us and contributes to implementing the concept of quality of life. It makes it easier for citizens to enjoy a way of living. The elderly for example, the IoT system can simplify their daily activities and provide the means by which they can access dedicated services in order to improve their quality of life [27]. The concept of "smart" makes you enjoy the benefit of being connected to the Internet. Smart city for example, promises to make city operation efficient while improving the quality of life for city inhabitants [28]. There has been a myriad of connected devices designed for services in all sectors that increased productivity and replace the human workforce [29].

On the other hand, unemployment is expected to spread, and many employees will stop performing their work and dispense with their services because of this development. The reengineering of works may result in the loss of jobs. Many of the jobs required today will stop, and it will become difficult to replace employees with new jobs. When people lose their jobs, they cannot enjoy anymore the life that they want to have. It is known that the IoTs and Artificial Intelligence projects came to make life easier, reduce costs, but they ignore people's employment [30].

In addition to the above, people will become lazier and more dependent in the presence of these advanced technologies to perform their tasks, which may result in many health problems, the first of

which is overweight and obesity. It may create health risks like repetitive stress injury that is caused by computer keyboards and also the Internet of Things creates the computer vision syndrome and finally the users of the IoT experience techno stress caused by the role of radiation, screen emissions and lastly it is caused by low-level electromagnetic fields. The negatives do not stop there, but it can also cause an increased dependence on the Internet in our lives. Psychological problems and the impact of social networks have many lessons.

Further, while IoT applications contribute to the quality of life, care should be taken to preserve not only value of life but also the cultural values and practices of the society. Measures should be taken to protect them from violation. Strictly, how the issues of equity, access and boundaries are observed and any actions and decisions that can prejudice the quality of life has moral decadence and ethical. Simply, the creation of the IoT may have implication to the negative social consequence of the systems. It means that the balance of power should be recognized, it should not be abused to the extent that it can destroy and hamper our enjoyment for the kind of life that we want to live with.

Nevertheless, we also recognize that in the balancing of power, the computing power is decentralized, and the key decision-making remains centralized. Other than balancing power, there is the rapidity of change where businesses may not have time to respond to global competition. Another issue relative to quality of life is on how to maintain boundaries where computing and the Internet use lengthens workday, personal time and infringes on family.

Additionally, there is that issue of vulnerability where private and public organizations are dependent on computer systems. Another crime that can possibly be committed would be the computer crime and abuse. As regards the computer crime, commission of illegal acts can happen through the use of a computer or against a computer system. This happens when the computer may become an object or instrument of the crime like the abuse of computer use but computer abuse may not be unethical or illegal as well.

In the UAE, quality of life is always preserved but welcoming the newest technology like the IoT comes not without the cost. The UAE has not issue related to the IoT equity and access and also about the balancing of power. With the economic development and the creation of the knowledge-based economy, it is inevitable for the country to embrace the IoTs but with it comes the price of ethical/moral, social and political issue but the country is prepared to sustain the quality of life that it used to enjoy ever since.

### 3. Discussion

It is clear by now that the IoT is a sought-after technology and pervasive that has already become widespread globally. The UAE is one of the countries that has vision into transforming to digital and becoming smart. Dubai is one of the cities around the world that is classified as a smart city. IoT is part of those smart systems that have been deployed around the world and continue to do so.

Unfortunately, the IoT have raised ethical, social and political issues. In order to reap the full benefit of the IoTs, measures should be taken in line with the development of all IoT in terms of technologies and regulation.

IoT ecosystems generate data and information which is prone to privacy breaches and security requiring measures to be taken. Scholars have suggested solutions and frameworks to counter these flaws in the IoT. For example, [31] proposed a flexible trust-aware access control system for the IoT, which provides an end-to-end and reliable security mechanism for the IoT devices, based on a lightweight authorization mechanism and a novel trust model that has been specially devised for IoT environments. Another example, [14], proposed techniques with architecture for preservation of data to ensure end-to-end privacy across the layers of the IoT ecosystem.

In the UAE, the growth of the IoT continue to transform the lives of every individual and the businesses as well for the better. Yet the government acknowledges the challenges that includes the greater security and privacy-related risks. The increased number of connected devices as the main feature of the IoT comes not without the costs. The UAE is aware of the effective and ethical use of the IoT to benefit especially the individuals, groups, institutions, and businesses. Simply, it explains that individuals in this country, which includes the businesses when it comes to the Internet of Things have the right to information and yet coupled with that right is their obligation to use ethically the information the individuals and businesses owned. Also, the same individuals, groups and businesses have the right to property or to possess intellectual property but at the same time, they have the moral obligation to make use of that intellectual right to benefit other individuals, groups and enterprises. Further to these moral dimensions is the accountability and control. It means every individual and business has the right to send or transmit the information and at the same to receive them and or both, but everyone must be accountable to the proper use of those information. In the case of the country, to avoid the possible crime related to this dimension, the government for its part must have an in-place

accountability and control management system. In this connection, the UAE Telecommunication Regulatory Authority (TRA) has recently laid its groundwork for regulating the IoT by introducing the IoT Policy. Also, the government sets a regulatory IoT procedure that gives the TRA control and oversight of the entire IoT services in the country. In addition, the UAE government sets forth some data-protection related principles. This is in connection with those IoT services within the UAE market that they should fully understand their obligations and accountability under the TRA's IoT policy and IoT procedures and going forward. The UAE IoT Policy and Procedures apply to all public authorities, individuals, companies, and other legal entities concerned with the IoT within utilization in the UAE. This likewise includes the IoT Service Providers that are operating within the UAE as well as with those foreign-based IoT Service Providers providing services in the remote UAE market.

Another moral dimension that governs the creation of the IoT is the System Quality. The UAE government desires that software and hardware to facilitate quality inter connectivity must be of quality to deliver effective and efficient services for individuals and businesses. Systems that are poorly created will negatively affect the kind of services especially for businesses which in return can adversely affect their business processes to the disadvantage of customers.

Finally, the most important moral dimension of the IoT is the preservation of the quality of life of every Emirati people. Although it is inevitable that the government is welcoming the newest IoT technology, yet the government believes that while there are some challenges and risks brought about by the IoT, yet the country believes that the benefits of the IoT are enormous as compared to the challenge's effects of them to the individuals, groups and businesses.

#### 4. Conclusion

The Internet has evolved greatly, and its role is no longer limited to browsing information, and using written, audio, and visual communication services, but rather to the possibility of connecting things to each other by connecting them to the network, and receiving and sending commands to remote devices through it. This is what has been termed the "Internet of Things".

In the UAE, the IoT has been growing in popularity. The country is aware of the repercussions when it comes to the possible issues related to application of the IoT and the possible crimes that can surface due to abusive users of this newest technology advancement. Also, with the growth of the IoT,

ethical and moral issues, political and social as well, challenge everyone including the individuals, groups, businesses, and enterprises. The welcoming of the IoT is not without risks and issues to reiterate and therefore the UAE as early as 2019 already imposed the IoT policies and procedures to regulate the use of the IoT. The five moral dimensions were used as the basis to govern the effective and efficient use of the IoT and to harness its full benefits by individuals, public authorities, institutions, and enterprises. Finally, it is argued that the IoT has also its weaknesses, risks, and challenges but it is claimed by various literature that the enormous benefits of the IoT outweigh its disadvantages especially in today's strong Internet connectivity.

#### References

- [1]. Ashton, K. (2009). That 'internet of things' thing. *RFID journal*, 22(7), 97-114.
- [2]. Ahmad, G. (2016). Internet of things (iot): An overview. *Journal of Information & Communication Technology (JICT)*, 10(1), 10.
- [3]. Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature. *Journal of Computer and Communications*, 3, 164-173.
- [4]. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15), 2787-2805.
- [5]. Davis, G. (2018, January). 2020: Life with 50 billion connected devices. In *2018 IEEE international conference on consumer electronics (ICCE)* (pp. 1-1). IEEE.
- [6]. Lefèvre, A. & Lefèvre, C., (2017). Internet of things: intellectual property focus for the protection of connected devices – IP & Entertainment Law,. *International Bar Association*.
- [7]. Alsaadi, E., & Tubaishat, A. (2015). Internet of things: features, challenges, and vulnerabilities. *International Journal of Advanced Computer Science and Information Technology*, 4(1), 1-13.
- [8]. Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety and ethics. In *Digital twin technologies and smart cities* (pp. 123-149). Springer, Cham.
- [9]. Allhoff, F., & Henschke, A. (2018). The internet of things: Foundational ethical issues. *Internet of Things*, 1, 55-66.
- [10]. AboBakr, A., & Azer, M. A. (2017, December). IoT ethics challenges and legal issues. In *2017 12th International Conference on Computer Engineering and Systems (ICCES)* (pp. 233-237). IEEE.
- [11]. Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, 82(2), 85-105.
- [12]. Ghandour, A., & Woodford, B. J. (2019, December). Ethical Issues in Artificial Intelligence in UAE. In *2019 International Arab Conference on Information Technology (ACIT)* (pp. 262-266). IEEE.

- [13]. Laudon, K.C. & Laudon, J.P., (2017). *Management Information Systems: Managing the Digital Firm, Global Edition*. Pearson.
- [14]. Jayaraman, P. P., Yang, X., Yavari, A., Georgakopoulos, D., & Yi, X. (2017). Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation. *Future Generation Computer Systems*, 76, 540-549.
- [15]. Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, 2(2), 155-184.
- [16]. Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer law & security review*, 26(1), 23-30.
- [17]. Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2015, September). On the security and privacy of Internet of Things architectures and systems. In *2015 International Workshop on Secure Internet of Things (SIoT)* (pp. 49-57). IEEE.
- [18]. Cam-Winget, N., Sadeghi, A. R., & Jin, Y. (2016, June). Can IoT be secured: Emerging challenges in connecting the unconnected. In *2016 53rd ACM/EDAC/IEEE Design Automation Conference (DAC)* (pp. 1-6). IEEE.
- [19]. Losavio, M. M., Chow, K. P., Koltay, A., & James, J. (2018). The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. *Security and Privacy*, 1(3), e23.
- [20]. Karadbhajne, H. & Shbham, R., (2019). Internet of Things (IoT) and Intellectual Property - The Interconnect. *S.S RANA & Co. Advocates*. Retrieved from: [https://www.ssrana.in/articles/internet-of-things-iot-and-intellectual-property-the-interconnect/?utm\\_source=Mondaq&utm\\_medium=syndication&utm\\_campaign=LinkedIn-integration](https://www.ssrana.in/articles/internet-of-things-iot-and-intellectual-property-the-interconnect/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration) [accessed: 27 March 2021].
- [21]. Janeček, V. (2018). Ownership of personal data in the Internet of Things. *Computer law & security review*, 34(5), 1039-1052.
- [22]. Scheibner, J., Jobin, A., & Vayena, E. (2020). Ethical Issues with Using Internet of Things Devices in Citizen Science Research: A Scoping Review. *Cambridge Handbook of Life Science, Information Technology and Human Rights*.
- [23]. Lindqvist, J. (2018). New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?. *International journal of law and information technology*, 26(1), 45-63.
- [24]. Crabtree, A., Lodge, T., Colley, J., Greenhalgh, C., Glover, K., Haddadi, H., ... & McAuley, D. (2018). Building accountability into the Internet of Things: the IoT Databox model. *Journal of Reliable Intelligent Environments*, 4(1), 39-55.
- [25]. Urquhart, L., Lodge, T., & Crabtree, A. (2019). Demonstrably doing accountability in the Internet of Things. *International Journal of Law and Information Technology*, 27(1), 1-27.
- [26]. Banerjee, T., & Sheth, A. (2017). Iot quality control for data and application needs. *IEEE Intelligent Systems*, 32(2), 68-73.
- [27]. Miori, V., & Russo, D. (2017, June). Improving life quality for the elderly through the Social Internet of Things (SIoT). In *2017 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE.
- [28]. Chakrabarty, S., & Engels, D. W. (2016, January). A secure IoT architecture for smart cities. In *2016 13th IEEE annual consumer communications & networking conference (CCNC)* (pp. 812-813). IEEE.
- [29]. Mähler, V., & Westergren, U. H. (2018, September). Working with IoT—a case study detailing workplace digitalization through IoT system adoption. In *IFIP International Internet of Things Conference* (pp. 178-193). Springer, Cham.
- [30]. Frank, M. R., Autor, D., Bessen, J. E., Brynjolfsson, E., Cebrian, M., Deming, D. J., ... & Rahwan, I. (2019). Toward understanding the impact of artificial intelligence on labor. *Proceedings of the National Academy of Sciences*, 116(14), 6531-6539.
- [31]. Bernabe, J. B., Ramos, J. L. H., & Gomez, A. F. S. (2016). TACIoT: multidimensional trust-aware access control system for the Internet of Things. *Soft Computing*, 20(5), 1763-1779.