Privacy and security challenges and opportunities for IoT Technologies during and beyond COVID-19

V. Bentotahewa, M. Yousef, C. Hewage, L. Nawaf and J. Williams

School of Technologies, Cardiff Metropolitan University, Cardiff, United Kingdom.

Abstract: The prevailing COVID-19 pandemic has put IoT based technologies to the test. It has given rise to diverse predictions for the future, and the expectations are that IoT inspired technologies will play a significant role in the new normal. However, one of the key challenges for the success of IoT is its privacy and security issues. This chapter presents a comprehensive review of privacy and security challenges and opportunities for IoT inspired solutions. Also, it provides an in-depth analysis of IoT inspired Big Data issues, data protection, and security concerns around IoT. The contributions of this chapter cover a comprehensive review of the IoT privacy issues and data protection policies, regulations, and laws, IoT security challenges and opportunities that need to be addressed in the next normal.

Keywords: Internet of Things, Privacy, Security, Big Data, Data protection, GDPR, COVID-19

1. Introduction

The Internet of Things (IoT) technology sees extensive growth with the increased number of smart devices connected via the Internet. The global market for IoT solutions is expected to grow to around 1.6 trillion USD by 2025 [1]. These predicted trends will give rise to the expansion of opportunities created by the COVID-19 pandemic. The IoT solutions such as remote health monitoring, and contact tracing enabled authorities to successfully manage the spread of the Coronavirus. However, wider deployment of IoT inspired technologies face challenging obstacles such as privacy and security concerns. This chapter uptakes a comprehensive review of these challenges and an in-depth analysis of the issue.

1.1 IoT role during COVID-19 pandemic

Coronavirus disease 2019 (COVID-19) is an infectious illness caused by a novel and newly discovered Coronavirus [2][3]. Some symptoms

of the disease are shortness of breath, chest pain, and fever. On the 11th of March 2020, the World Health Organization (WHO) declared a global pandemic due to the COVID-19 outbreak. To reduce social contact during the pandemic, "some *businesses must remain closed or follow restrictions on how they provide goods and services.*" [4].

HARVARD Medical school has highlighted that in certain COVID-19 related heart injury patients, the initial symptoms might have occurred inseveral forms [5]. Those without previous underlying cardiac problems might remain healthy, whilst in others, Oxygen supply failure to heart muscles might cause heart damage. In the context of COVID-19, the contributory factor would be the imbalance between 'supply and demand' for Oxygen to the heart. In the process of stabilizing Oxygen levels in the body, IoT played a key role in efficiently managing the Pulse Oximeter, Nebulizers and Oxygen tanks.

IoT technology has been used extensively for many purposes across diverse sectors during the pandemic as was referred to earlier, and their applications and frameworks have enabled successful management of the pandemic. Prior to the onset of the COVID-19 pandemic, IoT had been linked to certain key areas or catch phrases such as SMART homes, self-driving cars, smart metering, etc. However, in the aftermath of the pandemic, IoT was put into effective use across a wide range of sectors for purposes such as contact tracing, retail, and hospitality. The key IoT sectors affected by the pandemic, the economic/social impact, Technology Readiness Levels (TRL) are discussed in [6]. An elaboration of the industries affected and the IoT solutions used during the pandemic is set out in the following subsections.

1.1.1 Affected industries

Different industries, such as the Hospitality sector and the Restaurant industry were affected by the COVID-19 pandemic. The knock-on effect was felt in small and medium enterprise sectors, and consequently, they were badly hit. For instance, 3% of restaurants remained permanently closed [7]; Tourism sector [8] because of travel restrictions and freedom of movement due to social distancing rules; Airline industry because of

operational changes in air travel and airports, and the Travel agencies for the same reasons; Agricultural sector [9], on which other sectors, mentioned above, depended on; the Retail industry on which the consumers relied on to sustain their livelihood[10]; Education delivery system switching to virtual distance learning [11]; Healthcare services overwhelmed by the virus and COVID-19 cases. These are some of the examples of the affected industries, and the IoT solutions applied are highlighted in each case. The selected industries were chosen based on the background knowledge of the authors and the reviewed articles [16-22].

1.1.2 IoT solutions

In the agriculture industry and with the use of sensors IoT based smart farms could survive. IoT smart farms allow data collection, tracking remote monitoring, and remote control. The use of IoT in agriculture makes factories more efficient, optimize treatment and input required, efficient water use, and will make the environment better [9]. By implementing IoT technologies such as drones and sensors we can monitor crop health, seed inspection, seed harvesting, and soil examination. The author in [12] proposes the use of immersive technologies and Information and Communications Technology (ICT) for remote end-user applications, also, to inform disruptive innovations.

The author in [13] describes how IoT devices can lead to a hassle-free post-checkout sanitization that eliminates human to human interaction and enabled service reconfiguration, based on customer preferences survey of consumer behaviour and predictions in the hospitality industry. In addition, improvements to workplace safety can be made by installing real-time alarms to alert emergencies. IoT can also be used to ensure maintenance of hygiene standards in the sales outlets (cleanliness of restaurant tables, sanitiser solution concentration, contactless payment and communication) and adherence to social distancing rules [14][15] to minimize the need for manual interventions. The use of IoT retail self-checkouts such as kiosks, IoT automated systems such as Amazon warehouse, and RFID inventory tracking can help limit interaction between humans, thereby avoiding, human error, excess staff numbers, and enhance supply chain management with inventory, delivery, and storage [16][17]. There are diverse types of IoT wearables and devices for contact tracing, temperature screening used in the healthcare industry to

ensure social distancing, accurate diagnosis, tracking, and health monitoring and provide exposure notification [18][19].

The figure (Figure 1) below provides a summary of IoT solutions that are used in different industries.

Figure 1: Key IoT Solutions during COVID-19 Pandemic

This review provides an in-depth understanding of the main IoT sectors that played a vital role in managing the global pandemic and their potential applications in the post-COVID-19 future. Authors expect the usage of IoT based technologies, and applications to increase significantly during the next normal, matching lifestyle patterns such as working from home, distance learning, telemedicine, that have emerged during the pandemic.

The potential for this technology is immense, but the challenges are likely to be equally immense. Amongst other concerning issues, energy requirements of these IoT devices, and privacy and security are key priorities for consideration [20][21][22]. However, there is a lack of COVID-19 pandemic relevant literature published on the issues touched upon earlier. Therefore, in the absence of informative literature, the primary focus of this chapter will be on privacy and security issues associated with IoT data collection (Big Data) and security challenges. Subsection 1.2 summarises the privacy and security challenges of IoT.

1.2 Privacy and security concerns of IoT

Since the Internet of Things (IoT) came to being, its applications and the range of connected devices has multiplied, and in parallel, the expanding usage of IoT also induces many technical challenges potentially threatening the security and privacy of IoT end-users. Therefore, there is an imperative requirement to put in place risk mitigating solutions, sooner than later.

In the IoT environment, whilst safeguarding online security remains a major concern and a challenge, preserving privacy will also remain a significant challenge needing added attention. As an example, the privacy of the IoT end-users could be at risk if personal data happens to be leaked to unauthorized persons, or even through a security breach in the IoT (devices). Such incidents would potentially allow the attacker access to IoT end-user data without being tracked or traced by (face recognition) security cameras located in smart homes. Given the heterogeneity of IoT connected devices and in-built vulnerabilities of hardware and software in some of them, safeguarding end-user privacy might face many security challenges [23].

There are reported studies focussing on the privacy and security challenges of IoT [20][21][22]. However, this chapter provides an in-depth analysis of these important challenges especially in the aftermath of COVID-19. The discussion in Section 2 of this chapter focuses on the large volume of information generated through IoT devices, the analysis of security and privacy challenges associated with Big Data, and the provision of legal and policy solutions to protect privacy for maintaining trust between the data subject and data controller. IoT threats, security challenges, and proposed solutions are discussed in Section 3 of this Chapter. In addition, the impact of COVID-19 and the role of IoT in different industries is highlighted at the end of Section 3.

1.3 Study Methodology

The aim of this study is to review the privacy and security challenges of IoT technologies for the next normal. The research objectives of this studyare listed below:

a. Identification and in-depth analysis of privacy and data protection challenges associated with Big Data generated via IoT Technologies

b. Analysis and discussion of security challenges for IoT technologies for next normal, and finally the identification and analysis of best practices and code of practices for IoT technologies

The review was carried out by using publicly available secondary data sources that explore and discuss different aspects of IoT technologies in diverse sectors. The main data sources used in this review are the SCOPUS library, Web of Science citation database, ACM library, IEEE Xplorer, Google Scholar and Researchgate. A number of keyword searches were used to find relevant studies and reviews necessary to answer the research questions of this study. An exclusion criterion was not used to provide a wider overview of the issue. In addition to the initial research by the authors, recommendations by previously published research, tutorials, surveys, and reviews were used to select the prominent privacy and security challenges to focus on in this study.

1.4 Structure of the chapter

This chapter is organized as follows: Section 2 discusses IoT vs Data protection; Security architectures are discussed in Section 3; Section 4 summarises the future privacy and security landscape for IoT. The conclusion of the study is provided in Section 5.

2 Data Protection vs IoT

IoT technology has been used widely during the COVID-19 pandemic for the purpose of mitigating and preventing the spread of the Coronavirus. These internet-connected devices did serve the purpose, but they also gave rise to an up surge of privacy and security risks associated with the collection of a large volume of data. Section 2 is dedicated to investigating IoT generated Big Data and what actions could be taken to protect them. Section 2.1 focuses on literature-based definitions for Big Data generated by IoT, associated threats, and the importance of protecting Big Data. The authors have dedicated section 2.2 to highlight the data protection challenges and existing solutions to overcome potential challenges. In section 2.3, the authors have flagged up relevant Data laws associated with Big Data in parallel with GDPR. Section 2.4 highlights policy mechanisms and their purpose in the context of Big Data.

2.1 Usefulness and security of Big Data generated by IoT

The question that is often asked by those who are not familiar with modern tech jargon is ‘what is Big Data’. To explain it in simple terms, it is a vast amount of information collected for understanding and decision-making purposes using innovative forms of information processing[24]. In professional literature, the definition of Big Data refers to, the volume of data collected, the variety of sources, the speed of analysis and interpretation that could be achieved through the analytical process [25]. Data collected in this way have the capacity to reveal information about individuals in terms of their habits, location, interests and a host of other personal information, and varying preferences that are stored in the systems for usage with ease. While there is no single definition of Big Data, the Information Commissioner's Office (ICO) believes that it is useful toregard Big Data as data which, due to several varying characteristics, is difficult to analyse using traditional data analysis methods [26].

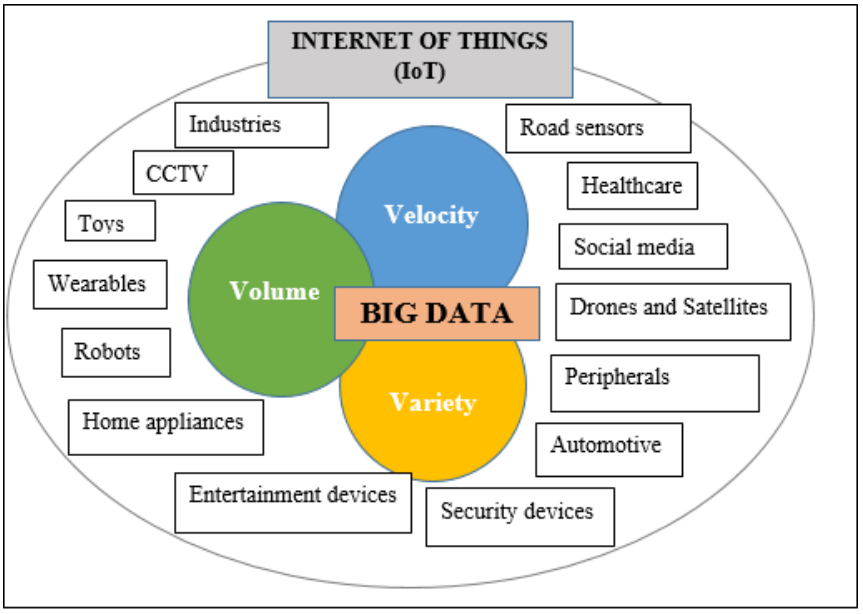
Big Data comes in various formats (Figure 02), such as cell phone location information, CCTV recordings, social media contents from a variety of sources and satellite images [27], and handling them is a

significant challenge. Primarily, data that relates to an identifiable living individual is considered as Big Data in (Article 4(1), General Data Protection Regulation (GDPR) [28], but not all the Big Data, for example, climate and weather data is not personal data [26]. Reports highlight the significant increase in the frequency of data breaches since 2015; 60% inthe USA only [29]. In 2016, the world was introduced to the security risks and vulnerabilities associated with smart technology aftermath of the Mirai IoT botnet Denial-of-Service (DoS) attack which caused widespread internet outages throughout the US and Europe [30]. Another report suggests that according to a survey conducted in Japan, Canada, the UK, Australia, the USA, and France has discovered that 63% of the IoT consumers thought these devices could not be trusted due to inadequate security [29]. Also, research findings have highlighted that 90% of consumers did not seem to have confidence in IoT cybersecurity [29].

There is no doubt that connected things in various sectors do bring tangible benefits that make life better, but also, they carry with them serious concerns about data security. There is no single magical solution to solve the identified Big Data security and privacy challenges. There are various challenges connected with data collecting, processing, and storing. Vast volumes of data become irrelevant unless they are processed to get something useful out of them. Therefore, it is important to ensure that the sensors function properly and the quality of the data coming for analysis is reliable, and not spoiled by factors such as environmental conditions, and sensor malfunction/breakdown.

Security of Big Data and privacy is an essential element that will ensure data trustworthiness in the data collection process and usage. In general, the majority of data breaches and IoT attacks happen due to a lack of user awareness [31] [29]. Therefore, documented user guidelines should be compulsory to strengthen security awareness. It has been reported that IoT security measures and guidelines had not been usually mentioned when the users purchased these devices [29]. To avoid any controversies, the device manufacturers ought to take the lead to bring potential IoT threats to the attention of the user, and the organisations should produce a package of effective training programs to enhance security awareness. In a positive move, in contrast, data protection authorities point out that, like any other form of data processing, Big Data falls within the framework of data protection law and must comply with data protection legislation

in accordance with GDPR which was established with technological advancements in mind.



Source: Authors, 2021

Figure 2. Generation of Big Data

2.2 Big Data protection challenges

In practice, data protection and security become extremely challenging in an IoT environment, as a communication interface between objects and persons is at the core of the system, without human intervention. Given the pace of change, it is not surprising that there is little evidence to presume that data protection is keeping up with the pace of change. Even though when legislative drafters demonstrate their awareness of specific concerns in processing data on a large scale, their understanding of risk implications may not be sufficient in practice.

Big data applications typically tend to collect data from diverse sources, without careful verification of the relevance or accuracy of the data thus collected [32]. Google's unsuccessful attempts at health diagnostic, and most recently, the use of analytics to predict the US election

results [33] can be taken as good examples of the inaccuracy of Big Data. On that basis, the accuracy principle can be challenged as the GDPR underscores the importance of accuracy [34] in personal data.

The GDPR applies to the processing of personal data, regardless of whether the processing takes place in the EU [35]. The controllers and processors and those acting as controllers of Big Data as well as those acting as processors on their behalf are obliged to comply with GDPR. The application of data protection principles could be challenging when using personal data in the Big Data context, especially where it involves the use of techniques made possible by AI. These implications arise not only from the volume of data but also from the ways in which data is generated, stored, and processed.

The creation of personal data in vast amounts through Big Data techniques allow organisations to combine different data sets, and that is likely to increase the capability of data to identify living individuals in new ways [36]. As a result, the capacity to mine and analyse datasets increases in volumes, variability, and velocity effectively giving rise to an exponentially increased volume of personal data. To overcome the challenges, in the context of Big Data, it is advisable to consider whether personal data can be fully anonymised. The GDPR specifies that the principles of data protection should not apply to anonymous information that does not relate to an identified or identifiable real person, or personal data classified 'anonymous' [37] in such a manner data subject's information is not protected under the GDPR. Therefore, organisations who use anonymised data are expected to verify that they had carried out a robust assessment of the risk of re-identification and adopted proportionate solutions [38]. This may involve a range of technical measures, such as data masking, pseudonymisation, aggregation and banding, as well aslegal and organisational safeguards [38].

The UK Anonymisation Network (UKAN) plays a significant role in providing expert advice on anonymisation techniques [39]. It also enables the organisation to reassure people that collected data capable of identifying them will not be used for Big Data analytics [38]. This is an important criterion for building trust and in taking Big Data forward. However, some commentators have made references to examples where it had been possible to identify individuals in anonymised datasets but

had concluded that anonymisation was becoming increasingly ineffective [38][40]. However, personal data that had been pseudonymised, in other words, identify an individual in conjunction with additional information could still be possible and will remain as classed personal data [26].

In the ICO Big Data Paper 2017, the ICO emphasises the importance of fairness, transparency, and the need for meeting the data subject's reasonable expectations in Big Data processing [40]. However, as vast amounts of data are processed through massive networks daily basis, there is limited transparency in how these algorithms work and how data is processed. Furthermore, the ICO Big Data Paper 2017 notes that the complexity of Big Data analytics can lead to mistrust and potentially be a barrier to data sharing, particularly both in the public and the privatesector. This can lead to reduced competitiveness as a negative perception of the consumer will impact trustworthiness. [26]. Therefore, in the Big Data context, privacy notices [41] serve as an important means of providing transparency, while also the consent factor [42] has been the most reliable in ensuring transparency. The ICO Big Data Paper 2017 makes itclear that the complexity of Big Data should not be taken as an excuse for failing to obtain consent if and when required to do so [40]. The GDPR also follows this approach by asserting that data processing is conditional onobtaining prior consent from the data subject [42]. However, the assertion to obtain consent for processing might not turn out to be a workable solution in all circumstances because of the complexity of the analytics. A study in the US suggests that companies overestimate customers' concerns about the use of their personal data. It claims that in reality, people are primarily concerned about what the organisations plan to do with their data [38]. This leads to the point that personal security remains uppermost in their thinking. Then it is arguably clear that emphasis should be on the data collection process and use rather than focusing on controlling what happens after data is collected. Therefore, where an organisation is relying on consent in the Big Data context, people must have an understanding of how the organisation will use their data, and aclear indication of consent given for the intended purpose only. To determine the intended purpose compatibility of data originally collected and used will increasingly become challenging with Big Data. If an organisation had collected personal data for one purpose and then decided

to start analysing for completely different purposes, the users need to be made aware of the changes and, where necessary, further consent needs to be obtained.

Connected things generate terabytes of data, therefore, deciding which data to store and which to drop is a demanding task in data minimisation. The custodians of stored data may need to retain them for use over a long period for use in the future. The challenge is to secure critical data from criminals and unauthorised access. Any breaches will compromise the privacy of the users and have a negative impact on the image of the custodian, affect trustworthiness, and the users will lose faith not only in the organisation but also in the system. According to an assumption that emerged in 2006, there were notable concerns about invasion of privacy amongst the adult population than the younger generation who felt comfortable about revealing their personal information [43]. But there had been proposed changes and the Oxford Internet Institute had released a report, in which it had stated that young people were found to be more likely to take action to protect their privacy than the elderly [43].

The principle of data minimisation is set out in Article 5(1)(c) – per personal data must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed [34]. Data minimisation therefore fundamentally collides with the concept of Big Data, which involves collecting as much data as possible. In the context of data minimisation, questions arise whether the data is excessive and relevant. Therefore, it is important for organisations to be able to articulate at the outset theneed to collect and process specific datasets.

Furthermore, the GDPR states that personal data shall not be retained for longer than necessary after serving the purpose for which the data had been processed [34], however, this requirement is likely to face challenges in the context of Big Data. The GDPR does not specify exact timelines for data retention given that they are context-specific [34] and difficulties that may arise in relation to the storage limitation principle in Big Data analytics. Most importantly storage limitation principle may undermine the predictability of the future as algorithms can potentially compare current data with stored historical data.

The principle of purpose limitation [44] [45] is seen as a challenge to Big Data and a barrier to the development of Big Data analytics in the absence of clarity of the purpose for which the data will be used. Also, there

has been suggested that the purpose limitation principle restricts freedom the organisations need to make discoveries and innovations happen, and the blunt statement that collection of data for big data analytics without a purpose does not stand to reason.

A privacy impact assessment [46] is also an important method that can help identify and mitigate privacy risks prior to the processing of personal data in any Big Data scenario. The unique features of Big Data can make some aspects of a privacy impact assessment additionally difficult, but these challenges can be overcome. The impact assessment of complex data collection and processing systems should be conducted by a third party under the supervision of national data protection authorities, that define the professional requirements of these third parties to produce unbiased, high standard outcomes [47].

Looking at the potential challenges clearly privacy remains is a major in the IoT, therefore, the service providers have a responsibility to respect consumer privacy by maintaining trustworthiness. That is a consumer-friendly essential to allay public fears when adopting new technology. Research suggests there will be 75 billion internet-connected devices, in homes around the world by the end of 2025 [48]. The individuals are likely to be unaware of the processing of their personal data collected using IoT applications. There are only a few IoT-related policies and regulatory frameworks currently in place, therefore, an effective law implementation mechanism is required to protect millions of users who will otherwise fall victims to cyber-related threats and hacks linked to internet-connected household items. The table (Table 01) below provides a summary of identified challenges and proposed solutions.

Table 01: Identified challenges and proposed solutions

Challenges	**Proposed solutions**
Collection of data from diverse sources, without careful verification of the relevance or accuracy [32].	Use AI technologies to verify the accuracy of collected data.
Big Data techniques allow organisations to combine different data sets, and that increases	Use of a wide range of technical measures, such as data masking, anonymization, pseudonymisation,

the likelihood of data being capable of identifying living individuals [36].	aggregation, as well as legal and organisational safeguards [38].
Limited transparency in how data is processed [38].	Improve transparency by providing privacy notices [41] and obtaining consent [42] before processing any collected data.
The complexity of Big Data analytics can lead to mistrust [26].	Improve transparency by providing privacy notices [41] and obtaining consent [42] before processing any collected data.
The challenge of determining which purposes are compatible with the purpose for which the data was originally collected.	Purpose limitation [44][45]; If an organisation has collected personal data for one purpose and then decided to start analysing it for completely different purposes, then the users need to be made aware of the changes and, where necessary, further consent needs to be obtained.
The custodians of stored data may need to retain them for use over a long period for use in the future.	Use of technical measures, such as anonymization and pseudonymisation [38].
Any breaches will compromise the privacy of the users and have a negative impact on the image of the custodian, affect trustworthiness, and the users will lose faith not only in the organisation but also in the system.	Use of technical measures, such as anonymization, pseudonymisation, data masking, encryption keys and blockchain technology. Physical security systems such as access control, use of video surveillance and security logs can also be used.
Protection of privacy of individuals.	Conducting privacy risks assessment will provide an early warning

	system to detect privacy problems [46].
Lack of IoT-related policies and regulatory frameworks at the national, regional and global level.	It is important to bring, countries, multinational organisations, industrial partners, security and IoT specialists from the industry and academia, to build dialogues on how to protect personal information generated through IoT. That will enable us to get a balanced view to move forward in developing policies and regulations associated with Big Data.
Principles in national and re-regional laws contradict with advancement of technologies.	It is important to review the policies at least twice a year to make sure there is a balance between upcoming technologies and legal mechanisms to protect the privacy of individuals and national security.

2.3 Emerging laws and regulations of data protection in IoT

Legal regulation is of increasing importance for Big Data, particularly for data protection. In this context, the application of established and developing data protection techniques are rapidly evolving. The managing of compliance with the GDPR will play an essential part in the Big Data handling projects involving data harvested from the expanding range of available digital sources. Many organisations do have established data protection governance structures and, policy and compliance frameworks in place, and these act as pathfinders towards Big Data governance.

The GDPR has recognised the rapid technological developments and globalisation with a special reference to Big Data technology [49], therefore, has provided further opportunity for regulators and organisations to consider Big Data compliance. In particular, the GDPR has introduced specific tools, like privacy by design [50] and pseudonymisation [51], to

help deal with Big Data. Consequently, the ICO [52] and other data protection authorities have been addressing Big Data for some time by further developing existing tools like notice and consent, anonymisation and privacy impact assessments in line with GDPR [52].

The Government of the United Kingdom recently launched a consultation process for regulating consumer Internet of Things (IoT) security, UK will be one of the first countries to legislate specifically in relation to IoT security, and other countries are likely to follow the UK model [53]. The UK government has proposed designating a regulator to monitor industry compliance. The proposals included civil enforcement powers, such as fines potentially up to 4% of annual worldwide turnover and product forfeiture, suspension, and recall. However, the omission of Wi-Fi security, as has been reported, would have a significant impact on general IoT security [53].

The EU Cyber Security Act 2019 initiated the development of a comprehensive cybersecurity certification schemes across the EU, but the US has so far failed to pass any federal legislation that will match the UK proposal [53]. The Government of UK is engaged with international partners to ensure that the guidelines drive a consistent, global approach to IoT security. As a step forward, in February 2019, ETSI, a global standards organisation, published the first globally applicable industry standard consumer IoT security, based on the UK Government's Code of Practice [48].

The UK government introduced a self-regulatory Code of Practice in October 2018 (CoP), and proposed to widen IoT devices related requirements, which included a ban on universal default passwords in IoT products, implementation of the vulnerability disclosure policy, and provision of a defined support period in terms of receiving security updates [53]. The proposals covered both producers and distributors, and the intended purpose was for all IoT devices sold in the UK to be compliant with the security requirements, including goods imported from elsewhere [53]. The included obligations were to ensure that all IoT devices met the security requirements, maintain thorough records of compliance, and cooperate fully with the regulator.

In January 2020, the UK government announced it was going to introduce new mandatory requirements for IoT device manufacturers for the purpose of improving consumer data security [54]. The aim was to

ensure these products had strong cybersecurity built-in by design and move responsibility to secure their own devices away from the consumers [54]. The three main requirements included were, unique passwords compulsory for all connected devices, provision of a point of contact for the public to report vulnerabilities, and a minimum period of security updates specified when sold [54].

In places where devices and services process personal data, the custodian should do so in accordance with applicable data protection law, such as the General Data Protection Regulation (GDPR). The emphasis should be for the individuals to remain in control of their personal data that are collected through IoT. In real circumstances, obtaining consent from the users may not be easy. Therefore, the device manufacturers and IoT service providers should make users aware of the way their data is being used, by whom, for what purposes, and clear instructions on how to delete their personal data for each device and service [34]. In cases where the data is being kept for a longer period than needed [34], all the credentials should be stored securely within services and on devices by using techniques like cryptographic keys, device identifiers and initialisation vectors [55]. In addition, significant sanctions for violations of data protection obligations should be introduced and, mandatory personal data breach notifications should be extended to all areas of personal data processing [56].

To ensure the implementation of data protection legislation by professionals, the role of data protection officers should be mandatory [57]. Inaddition to ensuring a high level of compliance, data protection officers themselves can provide data protection education to staff and management of their respective companies. Therefore, they could play an important role in the design of IoT systems by sharing their expert knowledge on data protection with relevant actors.

The proposals seek to protect the privacy of consumers and online security. The emphasis is also on the urgent need to ensure strong cybersecurity built into smart products by design. According to the director of marketing, the concerns over weak IoT security act as a barrier to the delivery of real benefits to individuals and societies [48]. Therefore, tech UK has been supporting the government's commitment to legislate for integrating cybersecurity into consumer IoT products at the design stage [58].

2.4 Policies and standards landscape for IoT

The data protection aspects of Big Data have been addressed in a number of reports, guidance and policy documents issued at the national and international level over the past few years (Table 02). The report sign posted Big Data's direction of travel and articulated a focus on data solutions and Big Data as a key IT driver over the next two decades [26].

UK government 2013 strategy paper: Seizing the data opportunity: a strategy for UK data capability, presented a positive view of the UK's ability to seize the data opportunity [59]. It addressed privacy and data protection issues through a clear and pragmatic policy to ensure public trust in the confidentiality of their data while increasing the availability of data to maximise its economic and social value [59].

The Executive Office of the US President's May 2014 report: Big Data: Seizing Opportunities, Preserving Value [60], focused on the way in which Big Data will transform everyday life, and it considered Big Data and privacy both in the public and the private sector and concluded that the existing notice and consent approach to data privacy may have to be reviewed in the light of Big Data [60].

The European Commission's 2014 Communication publication: Towards A Thriving Data-Driven Economy [61] sets out a number of activities it considered necessary for the EU to be able to seize Big Data opportunities. This report includes a data-friendly legal framework and policies. The report states that policies on issues relevant to Big Data like data protection and security should lead to more regulatory certainty for businesses and create consumer trust in data technologies [61].

The European Data Protection Supervisor's 2014 [62] and European Data Protection Supervisor's 2015 [63] opinion on the challenges of Big Data. The EDPS 2015 emphasised that data protection law must continue to protect existing rights and values even in the context of Big Data [63]. In general, the EDPS has called on the EU institutions to use the reform of the EU data protection framework to strengthen the data protection mechanisms to protect personal privacy and secure personal information [26].

In March 2017, the ICO published an updated paper on Big Data, artificial intelligence, machine learning and data protection with GDPR compliance elements [40]. This updated paper refers to the GDPR where

relevant, but it is not intended to be a guide to the GDPR. In particular, the ICO presents six recommendations to help organisations achieve compliance which includes anonymisation, privacy impact assessments (PIAs), appropriate privacy notices, privacy by design, the development of ethical principles and auditable machine learning algorithms [40].

Big Data cannot be secured by way of policies and legal mechanisms only. The use of encryption keys is one effective way to protect Big Data. The practicality of using public key encryption for encryption of data also enables decryption using the private key by the recipient, without undermining privacy and security [64]. Physical security systems, on the other hand, have built-in the capacity to deny data centre access to strangers or staff members, restricted to their status [65]. Similarly, the use of video surveillance and security logs will serve the same purpose [65]. These methods will contribute to maintaining and preserving confidentiality, integrity, and generated data availability.

Companies should continually monitor and identify, and rectify security vulnerabilities in their own products, and services as a part of the product security lifecycle [55]. On identifying any disclosed vulnerabilities, prompt action should be taken on the organisations. The sharing of known or identified vulnerabilities with the industrial entities will enablethem to be best prepared for potential vulnerabilities in the future internet.

In the absence of any regulation, it is unlikely that privacy, data pro-protection and information security will be addressed meaningfully and adequately by the market. In developing, accepting, and implementing policies associated with IoT, careful consideration should be given to avoiding violation of human identity, human integrity, human rights, the privacy of the individual and the public. The control of personal data should remain in their hands. To ensure harmonisation of privacy to a high standard, data protection, and information security, the development of a binding global data protection framework for IoT is appropriate and desirable.

Table 02: Implemented mechanisms and their purposes

Mechanisms	Purposed
UK government 2013 strategy paper: Seizing the data opportunity: a strategy for UK data capability [59].	It planned to address privacy and data protection issues through a clear and pragmatic policy that ensures public trust in the confidentiality of their data, while increasing the availability of data to maximise its economic and social value [59].
The Executive Office of the US President's May 2014 report: Big Data: Seizing Opportunities, Preserving Value [60].	This report considered Big Data and privacy both in the public and the private sector and concluded that the existing privacy notice and consent approach to data privacy may have to be reviewed in the light of Big Data [60].
The European Commission's 2014 Communication publication: Towards A Thriving Data-Driven Economy [61].	The report states that policies on issues relevant to Big Data like data protection and security should lead to more regulatory certainty for businesses and create consumer trust in data technologies [61].
The European Data Protection Supervisor's 2015 [63].	The EDPS 2015 emphasised that data protection law must continue to protect existing rights and values even in the context of Big Data[63].
In March 2017, the ICO published an updated paper on Big Data, artificial intelligence, machine learning and data protection with GDPR compliance element [40].	This updated paper presents six recommendations to help organisations achieve compliance which include anonymisation, privacy impact assessments (PIAs),

	appropriate privacy notices, privacy by design, the development of ethical principles and auditable machine learning algorithms [40].
Use of encryption keys	The practicality of using public-key encryption (PKE) for encryption of data also enables decryption using a private key by the recipient, without undermining privacy and security [64].
Implementation of physical security systems	Physical security systems have the capacity to deny data centre access to strangers or staff members, restricted to their status [65].

3. Security Challenges and Opportunities for IoT solutions

The Internet of Everything (IoE) is the next step to IoT as it will connect data, processes, devices, and people via the Internet [66]. The frog- leap in these exciting technological advancements come with risks, challenges, and opportunities of their own. Most of these risks are security relevant issues that will have a significant impact on individuals, organizations, and governments in general. This section highlights a multitude of IoT security challenges and the proposed solutions.

3.1 Security challenges

Due to device differences, protocols, and services in IoT, there needs to be a set of standards and well-defined architecture with interfaces, data models, and protocols. There is a concern that many researchers are focused mainly on authentication and access control protocols. When IoT devices are connected for the first time and share identifying information many attacks can happen such as the man in the middle (MITM) attack. To this end, authors in [67] stated that cryptography applied by predefined identity management entities that can monitor the connection of devices is needed to prevent identity theft. IoT requires more devices that will switch the use from IPv4 to IPv6 which will require more bandwidth. The implementation of both IPv6 and 5G the new generation of communication for better speed also open the doors for more threats and challenges that need to be addressed.

Different features of IoT devices can create threats and security challenges [68]. A better understanding of these features can help us mitigate some of these issues and rely on the consequences for a better solution. Features such as mobility, interdependency, diversity, intimacy and many more bring different challenges and threats such as firmware vulnerabilities, storage, computing power, network attacks, policies and standards that require more research. It requires thorough investigations to identify the root causes of IoT threats and also to build pragmatic countermeasures (e.g., "*the real risk which may be involved behind these vulnerabilities in the industrial context needs further investigation in the future*" [69].

There are methods that use blockchain to ensure privacy and security [70]. Confidentiality, Authorization, Integrity, and Availability are

achieved by using symmetric encryption, shared keys, hashing, and limiting acceptable transactions by the device. This method could be manageable for low resource IoT devices however, it produces some delay. The delay and the extra overheads are insignificant compared to its security and privacy gains to some applications but critical in others. Also, there is a blockchain IoT system that manages keys using RSA public key [71]. In this work, private keys are stored in the devices and public keys are stored in Ethereum. The proposed idea was implemented in a small scale IoT system and only a few IoT devices were used. The system showed two weaknesses. The first is the time it requires for data transactions and the latter is the requirement for larger storage for light IoT devices. In terms of threat and security, prevention from DDoS attacks was the only mentioned security measure that the system could provide. Data encryption is used to limit security risks as they increase for both business and consumers in the IoT environment and studies show that using AES in the algorithm is faster than both HAN and RSA algorithms[72].

There are major forensic challenges that face the IoT domain as there is no reliable and documented tool to collect residual evidence [73]. The autonomous and real-time interactions with different IoT devices and nods make it difficult to collect, identify, and preserve evidence data. Identifying activities of different parties that can access IoT nods is a challenge with the lack of a proper authentication system.

As there are some solutions that can be implemented to mitigate the security concerns, "*there is a clear lack of performance evaluation and assessment in real-life scenarios. Furthermore, there is a conflict between protecting user privacy and the granularity of data access needed to provide better services. This raises the challenge of how to support consumer-specific privacy preferences while maintaining the same levelof service*" [74].

3.2 Proposed secure IoT architectures

There is no single architecture or model of IoT. The proposed layer models vary from a 3-layers model to a 6-layers model. Many technologiesare involved to create an IoT system such as RFID, WSN, cloud computing, and different network technologies. This may result in different IoT security and privacy challenges such as Unauthorized Access to RFID, Sensor-Nodes Security Breach, and Cloud Computing Abuse.

To mitigate the threats that the IoT technology faces, there should be a better understanding of the technology used, architecture, type of attacks and where they all meet.

Different IoT layering systems: the 3-layers approach used by [67][74] and [75] (Application, network, and perception layer). The 4-layers approachused by [69](Application, data processing, network, and sensor and actuators layer). The 4-layers approach used by [76] and [77] (Application, middleware, network, and perception layer). The 6-layers approach used by [78] (Business, application, middleware, network, perception, and coding layer). 3 layers approach used by [73] and [72] (Application, transport, and sensing layer).

Many studies present the threats and challenges that the IoT based on a layering system faces. There are different layering approaches which make it difficult to allocate the same problem from one layering system to another. This increases the complexity and the time needed to find a proper solution. Here, we used the simplest layering system (figure 3) to demonstrate the most essential factors in a simpler way.

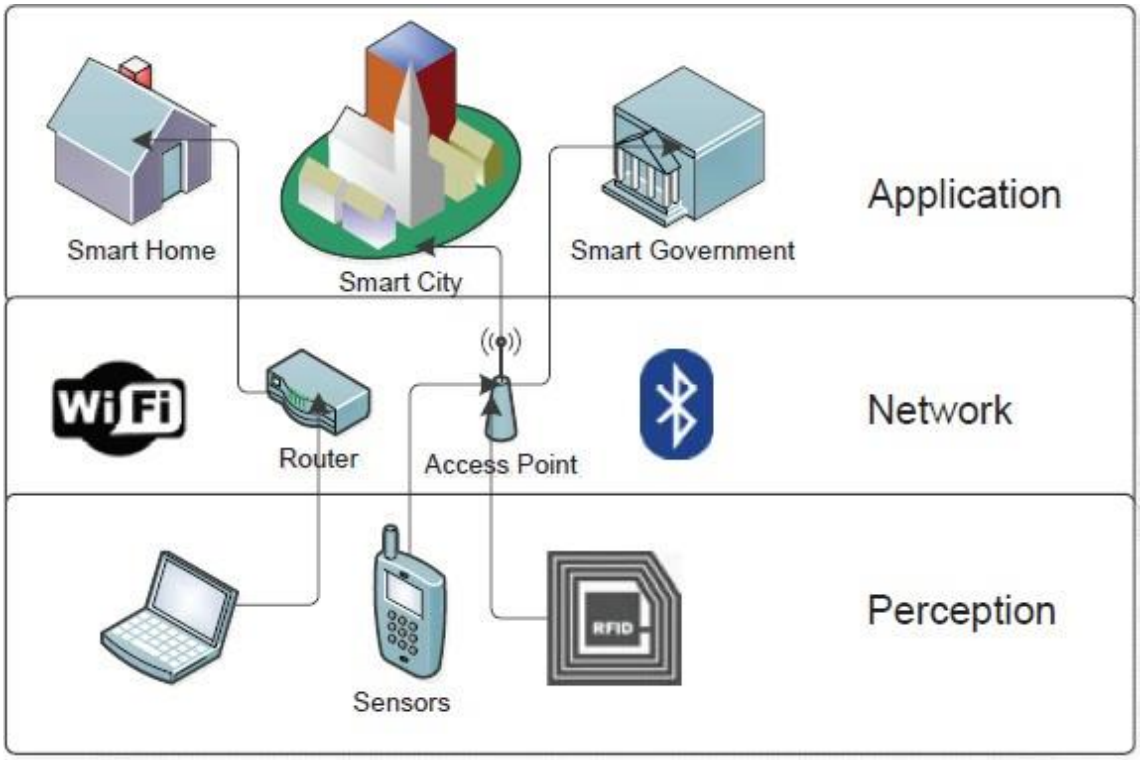


Figure 3 IoT layers [67]

First, the authors describe the most important technologies used in each layer bearing in mind that technology can be used in more than one layer. Figure 4 below provides a simplified example of some technologies used.

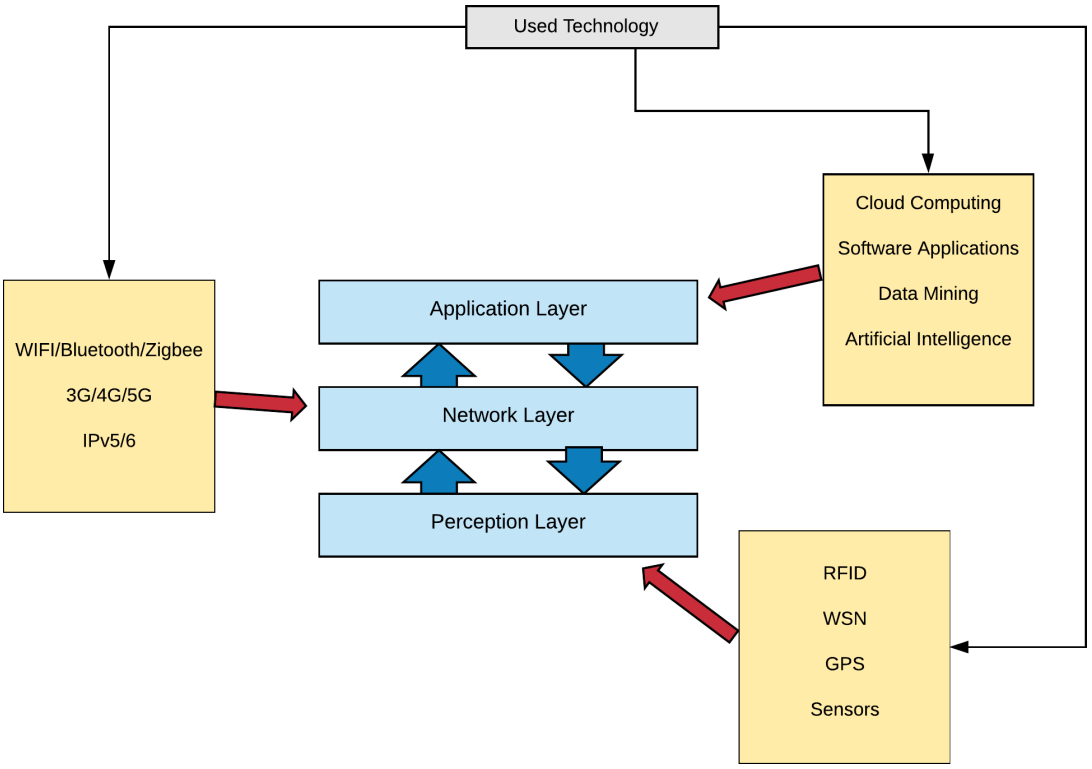


Figure 4 Used technologies in IoT layers.

In Figure 4, the authors explain different technology used in each layer. Threats can then be divided by the technology used rather than the layers they are in. This enabled authors to focus on the main technology used and how to implement the appropriate method to mitigate threats.

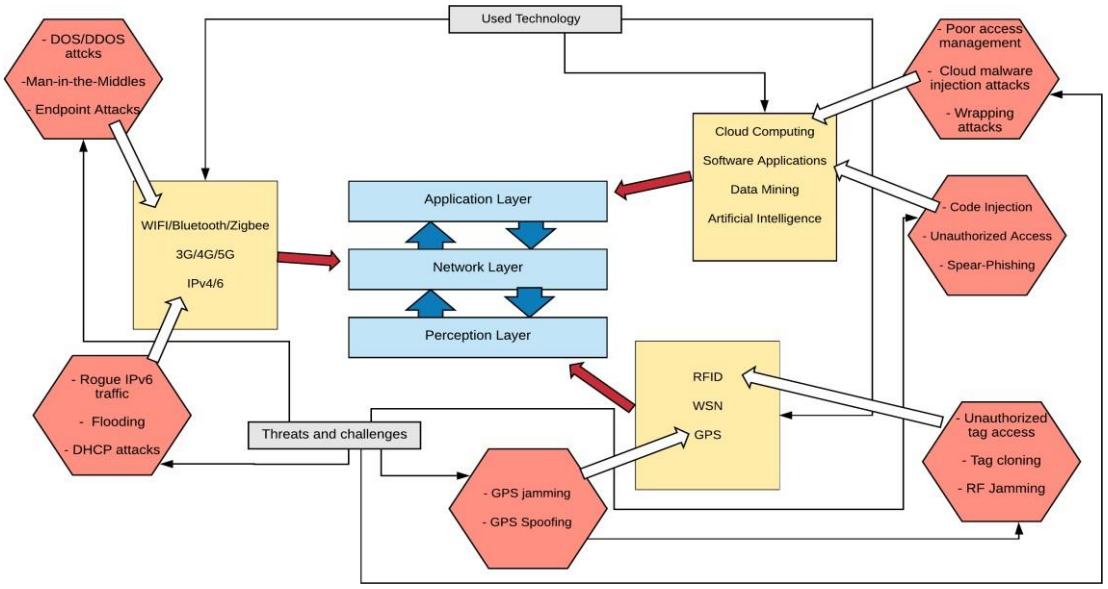


Figure 5 Threats on the used technologies

Figure 5 demonstrates risks associated with the used technology. This enables threats to be identified with ease. IoT systems do not facilitate all the technologies at once thus not all protection methods should be implemented. Protection and mitigation methods should be implemented based on the technology used. An example of this would be a system that uses either Bluetooth or Zigbee technology. Security implementation can be specific for the technology used rather than for all the options. This is very important for lightweight IoT devices because protection and security mechanisms tend to need more storage resources and computing power [68][69][71].

Table 3: Example of used technologies and their implementations

IoT Technologies	used/not used	Threats	Implementation
GPS	☐	- GPS Jamming - GPS spoofing	- Implement blocking antennas. - Obscure antennas
IPv4	☐	- DHCP Flooding	- Implement Port security
Cloud computing	☐	- Interception of Data	- Advanced web application firewalls - Data Encryption

An example of this would be listing the technologies that would be used in IoT rather than the layers in the model. Creating a manual or a table (such as Table 3) that lists all the used technologies, their threats and mitigation methods. In a simplified scenario, a company may need to create a new IoT device/application to serve a specific purpose. Users or researchers could first check all the technologies that will be used to create this tool (for example, not all the devices require cloud computing technology). Therefore, after an initial evaluation of the used technology, the appropriate control measures can be added to mitigate the threats associated with the technology. For instance, if GPS technology is used in the device, the "blocking antennas" method can be implemented as a control measure (refer to Table 3).

4. Future privacy and security landscape of IoT (post-COVID-19)

COVID-19 has made people work from home, shop online and students learn online. It is envisaged that these new normalcies will remain post COVID-19 as well. There are many privacy and security challenges associated with this new normalcy. Such challenges are not a phenomenon unique to the context of COVID-19. Yet both cyber threats and the enforcement gap were running at unacceptably high levels before the pandemic and have continued to do so throughout the crisis [79].

Even though the long-term impact of the COVID-19 crisis on the evolving threat of cybercrime cannot yet be assessed, there are several pressing questions about how the developments seen during the pandemic will affect the future privacy and security of people. Policymakers, practitioners, and advocates will have to come up with mandatory risk assessment frameworks to make sure the technology development companies will follow a strict risk assessment before they deploy any innovative technologies. This will prevent any security and privacy complications in the near future.

The response of the government and the technology industries to the Coronavirus outbreak became headlines news but at the same time, concerns were raised about the contact tracing apps, mobile location data tracking, and police surveillance drones [80]. Also, new privacy issues have emerged as the organisations started strengthening surveillance using thermal cameras and face-recognition technology in preparation for the resumption of normal working patterns. At one point during the pandemic, the WHO called the situation an Infodemic due to the increased collection of information [81]. According to the findings released from a survey conducted in the US, more than two-thirds of respondents believe that their government should be able to bring the virus under control without them having to sacrifice their privacy [82]. In this context, the governments, having to comply with the use of surveillance tools in combating the pandemic, should also need to strike a balance without compromising data privacy laws.

In a post COVID-19 world, we cannot expect the world to behave comparatively in the same manner as it did in pre COVID-19. It is extremely necessary to address privacy and security concerns during, and in post COVID-19. In doing so, the private sector can play an effective role in identifying cybercriminals and avoid disruptions to their infrastructure, but only the governments have the legal authority to prosecute and

bring them to justice [83]. Therefore, it is crucially important for the public and private sectors to work together on cybercrime issues. That having said, the possibility of some disparities in organisational culture and capacity between the institutions cannot be discounted.

As it stands, there is a clear visible gap in the development of IoT devices and regulatory laws do exist. Therefore, it is imperative to revisit national and regional data protection mechanisms to address upcoming potential threats, and it would be beneficial to capture data protection principles highlighted in the GDPR. The specific principles such as anonymisation, pseudonymisation, right to be erasure, obtaining consent before collecting and processing of personal information, deletion of collected data within a specified time scale, informing the data subject how the organisations will use their personal information. The adherence to these principles helps build a trustworthy relationship between data controllers and the data subject. However, some have opined that revisiting data protection laws and regulations such as GDPR will jeopardise the success of Big Data [84][85].

5. Conclusion

This chapter discusses the process of Big Data generated through IoT, the challenges and opportunities that have come to light during the COVID-19 pandemic. The authors have reviewed the conceptual meaning of 'BIG Data', and the process of generating a vast volume of data as the definition suggests. The nations have relied on technological solutions to minimise and contain the spread of the pandemic, and the increase in numbers of IoTs connected through the internet has generated vast volumes of information. As much as the outcomes are tangible and clearly visible, the focus has shifted to concerning security implications on personal privacy and security. In searching for solutions, the authors have identified the importance of accepting and implementing laws, regulations, and policies associated with IoT, with a special focus on GDPR. In this article, the authors have explored legal mechanisms already in place and have highlighted the importance of developing and revisiting national and regional data protection mechanisms. A consensus-based set of legislation in line with data protection principles highlighted in the GDPR is needed to confront future threats against personal privacy and security. Implementation of such policies and technical solutions will provide guidance and binding responsibility on the part of the manufacturers and organisations to protect the privacy of the individual whilst achieving the objectives of IoT deployment.

6. References

[1] Statista, “Forecast end-user spending on IoT solutions worldwide from 2017 to 2025(in billion U.S. dollars).” Statista. https://www.statista.com/statistics/976313/global-iot-market-size/ (Accessed 14 March 2021).

[2] W. H. Organization, “Coronavirus.” [Online]. Available: https://www.who.int/health-topics/coronavirus#tab=tab_1. [Accessed: 22-Apr-2021].

[3] “COVID-19.” [Online]. Available: https://apha.org/Topics-and-Issues/Communicable-Disease/Coronavirus. [Accessed: 22-Apr-2021].

[4] “(COVID-19) Coronavirus restrictions: what you can and cannot do - GOV.UK.” [Online]. Available: https://www.gov.uk/guidance/covid-19-coronavirus-restrictions-what-you-can-and-cannot-do#businesses-and-venues. [Accessed: 22-Apr-2021].

[5] E. Pesheva, “Coronavirus and the Heart,” 2020. [Online]. Available: https://hms.harvard.edu/news/coronavirus-heart (Accessed July 21, 2020).

[6] Yousif, M.; Hewage, C.; Nawaf, L. IoT Technologies during and beyond COVID- 19: A Comprehensive Review. Future Internet 2021, 13, 105. https://doi.org/10.3390/fi13050105

[7] H. J. Song, J. Yeon, and S. Lee, “Impact of the COVID-19 pandemic: Evidence from the U.S. restaurant industry,” Int. J. Hosp. Manag., vol. 92, 2021.

[8] F. Altuntas and M. S. Gok, “The effect of COVID-19 pandemic on domestic tourism: A DEMATEL method analysis on quarantine decisions,” Int. J. Hosp. Manag., vol. 92, 2021.

[9] P. K. Dutta and S. Mitra, “Application of Agricultural Drones and IoT to Understand Food Supply Chain During Post COVID-19,” in Agricultural Informatics, 2021.

[10] “COVID-19 and the retail sector: impact and policy responses,” 16 -Jun-2020. [Online]. Available: https://www.oecd.org/coronavirus/policy-responses/covid- 19-and-the-retail-sector-impact-and-policy-responses-371d7599/. [Accessed: 23- Apr-2021].

[11] G. Ilieva and T. Yankova, “IoT in Distance Learning during the COVID-19 Pandemic,” TEM J., vol. 9, no. 4, 2020.

[12] N. J. Rowan and C. M. Galanakis, “Unlocking challenges and opportunities presented by COVID-19 pandemic for cross-cutting disruption in agri-food and green deal innovations: Quo Vadis?,” Science of the Total Environment, vol. 748. 2020.

[13] S. G. Pillai, K. Haldorai, W. S. Seo, and W. G. Kim, “COVID-19 and hospitality 5.0: Redefining hospitality operations,” Int. J. Hosp. Manag., vol. 94, 2021.

[14] H. Suleman, “How to Use the IoT to Keep Your Restaurant Clean and Safe | FoodSafetyTech,” 12-Mar-2021. [Online]. Available: https://foodsafetytech.com/column/how-to-use-the-iot-to-keep-your-restaurant-clean-and-safe/. [Accessed: 22-Apr-2021].

[15] R. Embree, “Four IoT Trends for Hospitality | Hospitality Technology,” 19-Mar- 2021. [Online]. Available: https://hospitalitytech.com/four-iot-trends-hospitality. [Accessed: 22-Apr-2021].

[16] J. Panchal, “How IoT-enhanced warehouses are changing the supply chain management - Part 1 - IoT Now News - How to run an IoT enabled business,” 07-Jan-2019. [Online]. Available: https://www.iot-now.com/2019/01/07/91762-iot-enhanced-warehouses-changing-supply-chain-management/. [Accessed: 03-Mar-2021].

[17] “Self Checkout Systems in 2021: Comprehensive Guide,” 06 -Jan-2021. [Online]. Available: https://research.aimultiple.com/self-checkout/. [Accessed: 23-Apr-2021].

[18] Triax Technologies, “Proximity Trace » Triax Technologies.” [Online]. Available: https://www.triaxtec.com/resource/fact-sheet/proximity-trace/. [Accessed: 23-Apr-2021].

[19] “Covid-19 Temperature Screening Service & Test | Metro Security.” [Online]. Available: https://www.metrosecurity.co.uk/services/temperature-screening/. [Accessed: 23-Apr-2021].

[20] Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. Computers 2020, 9, 44. https://doi.org/10.3390/computers9020044

[21] Nazar Waheed, Xiangjian He, Muhammad Ikram, Muhammad Usman, Saad Sajid Hashmi, and Muhammad Usman. 2020. Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures. ACM Comput. Surv. 53, 6, Article 122 (February 2021), 37 pages. DOI:https://doi.org/10.1145/3417987

[22] Z. Berkay Celik, Earlence Fernandes, Eric Pauley, Gang Tan, and Patrick McDaniel. 2019. Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities. ACM Comput. Surv. 52, 4, Article 74 (September 2019), 30 pages. DOI:https://doi.org/10.1145/3333501

[23] Bertino, E., 2016, March. Data Security and Privacy in the IoT. In EDBT (Vol. 2016, pp. 1-3).

[24] Wu, X., Zhu, X., Wu, G. and Ding, W., 2014. “Data mining with big data,” IEEE Transactions on Knowledge and Data Engineering, 26(1), pp.97 -107. 2014. [Online]. DOI: 10.1109/TKDE.2013.109.

[25] Erevelles, S., Fukawa, N. and Swayne, L., “Big Data consumer analytics and the transformation of marketing,” Journal of Business Research, 69(2), pp.897 -904. 2016. [Online]. DOI: 10.1016/j.jbusres.2015.07.001

[26] K. Richard, “Big data and data protection (UK).” Practical Law. https://uk.practicallaw.thomsonreuters.com/w-017-1623?transitionType=Default&contextData=(sc.Default)&firstPage=true (Accessed 14 March 2021)

[27] Oussous, A., Benjelloun, F., Ait Lahcen, A. and Belfkih, S., “Big Data technologies: A survey,” Journal of King Saud University - Computer and Information

Sciences, 30(4), pp.431-448. 2018. [Online]. DOI: https://doi.org/10.1016/j.jksuci.2017.06.001
[28] Intersoft Consulting, "Art. 4 GDPR Definitions." General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-4-gdpr/ (Accessed 4 June 2019)
[29] Tawalbeh, L., Muheidat, F., Tawalbeh, M. and Quwaider, M., "IoT Privacy and Security: Challenges and Solutions," Applied Sciences, 10(12), p.4102. 2020. [Online]. https://doi.org/10.3390/app10124102
[30] J. N. Rosenthal, and D. J. Oberly, "The Rise of Internet of Things Security Laws: Part I" Pratt's Privacy & Cybersecurity Law Report (Vol. 6, No. 5). pp. 155 -158. 2020. [Online]. https://www.jdsupra.com/legalnews/the-rise-of-internet-of- things-security-50035/
[31] A Jurcut, T. Niculcea, P. Ranaweera, P. et al. "Security Considerations for Internet of Things: A Survey," SN COMPUT. SCI. 1, p.193. 2020. DOI: https://doi.org/10.1007/s42979-020-00201-3
[32] S Mortier, J Debussche, J César, "Big Data & Issues & Opportunities: Privacy and Data Protection." Bird and Bird. https://www.twobirds.com/en/news/articles/2019/global/big-data-and-issues-and-opportunities-privacy-and-data-protection (Accessed: 12 January 2021)
[33] Y. McDermott, "Conceptualising the right to data protection in an era of Big Data," Big Data & Society, 4(1). 2017. DOI: doi:10.1177/2053951716686994
[34] Intersoft Consulting, "Art. 5 GDPR Principles relating to processing of personal data." General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-5-gdpr/ (Accessed 12 June 2019)
[35] Intersoft Consulting, "Art. 3 GDPR Territorial scope." General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-3-gdpr/ (Accessed 16 June 2019)
[36] C. Brogan, "Anonymising personal data 'not enough to protect privacy', shows new study," Imperial Collage. https://www.imperial.ac.uk/news/192112/anonymising-personal-data-enough-protect-privacy/ (Accessed: 15 November 2019)
[37] Intersoft Consulting, "Recital 26 Not Applicable to Anonymous Data*." Recitals. https://gdpr-info.eu/recitals/no-26/ (Accessed 26 May 2019)
[38] Information Commissioner's Office. Big data and data protection. Version 1.0. P. 12-13. [Online] Available: https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220
[39] "UK Anonymization Network." https://ukanon.net/ (Accessed 23 March 2021)
[40] Information Commissioner's Office. Big data, artificial intelligence, machine learning and data protection. Version 2.2. P. 59. [Online] Available: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf
[41] Information Commissioner's Office. "What privacy information should we pro- vide?" https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the- general-data-protection-regulation-gdpr/the-right-to-be-informed/what-privacy- information-should-we-provide/ (Accessed: 17 March 2020)
[42] Intersoft Consulting, "GDPR Consent." General Data Protection Regulation (GDPR). https://gdpr-info.eu/issues/consent/ (Accessed 20 May 2019)

[43] C. Maple “Security and privacy in the internet of things,” Journal of Cyber Policy, 2:2, 155-184, 2017. DOI: 10.1080/23738871.2017.1366536
[44] Intersoft Consulting, “Art. 9 GDPR processing of special categories of personal data.” General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-9-gdpr/ (Accessed 10 September 2019)
[45] Intersoft Consulting, “Chapter 9 Provisions relating to specific processing situations.” General Data Protection Regulation (GDPR). https://gdpr-info.eu/chapter- 9/ (Accessed 15 September 2019)
[46] Intersoft Consulting, “GDPR Privacy Impact Assessment” General Data Protection Regulation (GDPR). https://gdpr-info.eu/issues/privacy-impact-assessment/ (Accessed 2 June 2019)
[47] A. Mantelero and G. Vaciago, “Data protection in a big data society. Ideas for a future regulation,” Digital Investigation, Volume 15. p.104 -109. 2015. [Online]. DOI: https://doi.org/10.1016/j.diin.2015.09.006.
[48] Department for Digital, Culture, Media & Sport, National Cyber Security Centre, and M Warman, “Government to strengthen security of internet-connected products,” https://www.gov.uk/government/news/government-to-strengthen-security- of-internet-connected-products (Accessed: 14 May 2020)
[49] Intersoft Consulting, “Recital 6 Ensuring a High Level of Data Protection Despite the Increased Exchange of Data*”Recital. https://gdpr-info.eu/recitals/no-6/ (Accessed 2 April 2019)
[50] Intersoft Consulting, “GDPR Privacy by Design” General Data Protection Regulation (GDPR). https://gdpr-info.eu/issues/privacy-by-design/ (Accessed 2 April 2019)
[51] Intersoft Consulting, “Recital 28 Introduction of Pseudonymisation*” Recital. https://gdpr-info.eu/recitals/no-28/ (Accessed 2 April 2019)
[52] Information Commissioner’s Office. “The UK GDPR” https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr (Accessed 24 November 2019)
[53] H. Beverley-Smith, C. H.N. Perowne and J. G. Weiss, “Internet of Things: How the U.K.’s Regulatory Plans Could Raise Compliance Standards,” The National Law Review, Volume XI, Number 104. 2020. [Online]. https://www.natlawreview.com/article/internet-things-how-uk-s-regulatory-plans-could-raise-compliance-standards
[54] A. Fernandez, “New IoT security regulations: what you need to know,” https://www.allot.com/blog/new-iot-security-regulations-what-you-need-to-know/ (Accessed: 12 April 2020)
[55] Department for Digital, Culture, Media & Sport, Code of Practice for Consumer IoT Security, United Kingdom: 2018. [Online]. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf
[56] Intersoft Consulting, “GDPR Fines / Penalties.” Key issues. https://gdpr-info.eu/issues/fines-penalties/ (Accessed 15 September 2019)

[57] Intersoft Consulting, “Art. 37 GDPR Designation of the data protection officer.” General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-37-gdpr/ (Accessed 15 September 2019)

[58] P. Muncaster, “UK’s IoT Law Hopes to Drive Security-by-Design,” infosecurity. https://www.infosecurity-magazine.com/news/uks-iot-law-hopes-to-drive/ (Accessed: 23 July 2020)

[59] Government of UK. Seizing the data Opportunity; A strategy for UK data capability, United Kingdom: Government publication, 2013. [Online]. Available https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/254136/bis-13-1250-strategy-for-uk-data-capability-v4.pdf

[60] Government of US. Big Data: seizing opportunities, preserving values, United State: Government Publication, 2015. [Online] Available https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf

[61] European Commission. Towards a thriving data -driven economy, Europe: European Commission. 2014. [Online]. Available https://ec.europa.eu/transparency/regdoc/rep/1/2014/EN/1-2014-442-EN-F1-1.Pdf

[62] European Union. European Data Protection Supervisor- Resolutions, recommendations and opinions, Europe: European Union. 2015. [Online]. Available https://ec.europa.eu/dorie/fileDownload.do;jsessionid=UdwG4bm1A8b_m1-1-UyfY02xUZ1JtAlxTYCJelGukIsnFGJyQCuC!-898031139?docId=2199637&cardId=2199636

[63] European Union. European Data Protection Supervisor; Annual Report 2015. Europe: European Union. 2015. [Online]. Available https://ec.europa.eu/dorie/fileDownloa d.do;jsessionid=UdwG4bm1A8b_m1 -1-UyfY02xUZ1JtAlxTYCJelGukIsnFGJyQCuC!-898031139?docId=2199637&cardId=2199636

[64] K. K. Pandey, Rammilan and D. Shukla, “Security and Privacy Challenges in Big Data,” Researchgate, pp74-77. 2018. [Online]. https://www.researchgate.net/publication/324482789_Security_and_Privacy_Challenges_in_Big_Data

[65] K. Rahfaldt, “How Leveraging Big Data Changes the Perception of Security,” https://www.securitymagazine.com/articles/90766-how-leveraging-big-data-changes-the-perception-of-security (Accessed: 22 February 2020)

[66] V. L. Kalyani and D. Sharma, “IoT: Machine to Machine (M2M), Device to Device (D2D) Internet of Everything (IoE) and Human to Human (H2H): Future of Communication,” J. Manag. Eng. Inf. Technol., no. 26, 2015.

[67] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, “Internet of things (IoT) security: Current status, challenges and prospective measures,” in 2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015, 2016.

[68] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, “The effect of IoT new featureson security and privacy: New threats, existing solutions, and challenges yet to be solved,” IEEE Internet Things J., vol. 6, no. 2, 2019.

[69] P. Varga, S. Plosz, G. Soos, and C. Hegedus, "Security threats and issues in automation IoT," in IEEE International Workshop on Factory Communication Systems - Proceedings, WFCS, 2017.

[70] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017, 2017.

[71] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in International Conference on Advanced Communication Technology, ICACT, 2017.

[72] A. Yousefi and S. M. Jameii, "Improving the security of internet of things using encryption algorithms," in IEEE International Conference on IoT and its Applications, ICIOT 2017, 2017.

[73] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," Future Generation Computer Systems, vol. 78. 2018.

[74] M. Seliem, K. Elgazzar, and K. Khalil, "Towards Privacy Preserving IoT Environments: A Survey," Wireless Communications and Mobile Computing, vol. 2018. 2018.

[75] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in 2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 - Proceedings, 2012.

[76] M. U.Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Int. J. Comput. Appl., vol. 111, no. 7, 2015.

[77] E. Leloglu, "A Review of Security Concerns in Internet of Things," J. Comput. Commun., vol. 05, no. 01, 2017.

[78] M. U.Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A Review on Internet of Things (IoT)," Int. J. Comput. Appl., vol. 113, no. 1, 2015.

[79] A. Peters, "Is COVID-19 changing the cybercrime landscape?," in The COVID-19 pandemic and trends in technology. Chatham House, 2021. [Online]. Available: ISBN: 978 1 78413 436 5.

[80] O. Holmes, J. McCurry and M. Safi, "Coronavirus mass surveillance could be here to stay, experts say." The Guardian, https://www.theguardian.com/world/2020/jun/18/coronavirus-mass-surveillance-could-be-here-to-stay-tracking (Accessed 4 February 2021)

[81] WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, "UN Global Pulse, and IFRC Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation." WHO. https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation (Accessed 18 December 2020)

[82] K. Lovejoy, "COVID-19: How future investment in cybersecurity will be impacted." EY Global Consulting. https://www.ey.com/en_gl/consulting/how-the-

covid-19-pandemic-is-impacting-future-investment-in-security-a nd-privacy (Accessed: 25 October 2020)

[83] Daniel, M. et al. “How do we beat COVID-19 cybercrime? By working together.” World Economic Forum, https://www.weforum.org/agenda/2020/07/alliance-tackling-covidclass="•-No-break">-19-cybercrime (Accessed 3 January 20221)

[84] T. Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 2017. [Online]. Available: https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1606&context=shlr

[85] S. Bentotahewa, C. Hewage, “Challenges and Obstacles to Application of GDPR to Big Data.” Info security. https://www.infosecurity-magazine.com/next-gen-infosec/challenges-gdpr-big-data/ (Accessed 23 January 2021)