Drivers and Challenges of IoT Diffusion in Smart Stores: A Field Exploration

Abstract

The digitally disruptive environment has evolved rapidly by introducing new advancements within the field of smart applications. Applications of one of the most prominent technologies, the Internet of Things (IoT), often appear in the retail sector, where smart services have transformed the customer experience holistically. In this paper, we present the findings from an exploratory field study in the retail services sector, drawing on the views of experienced practitioners about the smart store experience and the associated change. The study presents an overview of the drivers of smart retail service diffusion and the relevant challenges, such as business expectations and heterogeneity of devices respectively. The arising themes, indicate that IoT security is a major challenge for businesses installing IoT devices in their journey towards smart store transformations. The study highlights the importance of a secure data sharing IoT environment that respects the customer privacy, as the smart experience in store is about data-driven insight and services. Implications for research and practice are discussed in terms of the customer experience relevant to the identified challenges.

Keywords: Internet of Things; retail; smart store; security; privacy; diffusion of innovations; field study

1 Introduction

The cost-effective, accessible nature of IoT devices, combined with their ability to connect an organisation to both its environment and its customers in real-time, has made the technology highly attractive to a wide variety of industry sectors (Metallo et al., 2018). For example, it has been identified as one of the four leading disruptive technologies that will revolutionise the retail industry (Grewal et al., 2017.

At the same time, customer expectations began shifting from being product-centric to being more experiential (von Briel, 2018). On the one hand, the exponential development of the IoT makes it essential to cater to the quality expectations of end-users and monitor processes in an organisation. On the other hand, focusing on the experiential aspects requires the collection of unprecedented amounts of data and the use of advanced analytics (Bradlow et al., 2017). Given the customer-centric dynamic of a service environment, the potential volume of personal data that can be amassed is vast, thus bringing obvious implications for data privacy (Aloysius et al., 2018; Inman and Nikolova, 2017a). However, broader challenges, including security concerns, need to be considered (Marikyan et al., 2020). From a practical perspective, there is widespread acknowledgement that the simple increase of devices within a network poses a threat because it increases exposure to potential attacks (Jing et al., 2014; Roman et al., 2011). The heterogeneous nature of IoT devices further increases risks because it raises the degree of complexity regarding security requirements as IoT introduces computationally weak devices in an online environment which contributes to system vulnerability (Jing et al., 2014; Roman et al., 2011).

Recent advances in sensor networks and IoT and their widespread adoption and diffusion have helped facilitate monitoring and quality control processes. However, the translation of traditional security protocols onto an IoT system is inappropriate due to the differences between an IoT infrastructure and a 'traditional' computer network. Along these lines, and whilst the pool of academic research concerning the IoT (and IoT security) at both conceptual and a low, technical level is well populated, literature which addresses the IoT at a system level is relatively sparse (Boyes et al., 2018; Dijkman et al., 2015).

Addressing this gap, the present study explores the drivers and relevant challenges that organisations face when implementing an IoT system in smart stores, as well as the implications for the customer service experience. We address our research question: *"What are the drivers and challenges that companies face during the implementation of IoT in smart stores and which of them are relevant to the customer-facing services?",* by drawing from existing frameworks of service systems and the diffusion of innovations theory. Methodologically-wise, we build on a field study and combine a literature review with interviews with practitioners from the retail sector and expertise in implementing technology projects. Our findings contribute to the IoT literature by identifying the security facets that are specifically relevant to IoT in the retail service industry. We also offer practical implications that take the form of an agenda, providing feasible potential solutions for addressing IoT-related challenges, emphasizing the need to tailor these for a customer-facing service environment.

2 Prior Research

Over the past 20 years, the ambition of the IoT has transcended the idea to become a technology that pervades multiple aspects of modern life (Lee and Lee, 2015). The ubiquitous nature of IoT is discussed in Atzori et al.'s seminal study as a "variety of things or objects" that "through unique addressing schemes, are able to interact with each other and cooperate with their neighbours to reach common goals" (Atzori et al., 2010). The same authors identify RFID as being a key technology in the IoT moving forward and add that sensor networks, combined with RFID technologies, will further enable the digitalisation of the real-world environment. Given that the IoT leads to exponentially larger generation of data compared to traditional web-based technologies, utilising cloud technology is the only feasible way of storing, accessing and analysing information in a useful way (Gubbi et al., 2013). While there are challenges surrounding synchronisation and standardisation between different cloud vendors, reliability, management, and validating IoT cloud-based services, the cloud can still holds the potential to manage big data generated from the IoT (Al-Fuqaha et al., 2015).

Overall, the advancement of IoT can enhance the quality of the everyday customer experiences (Whitmore et al., 2015). However, as these technologies become sophisticated and pervasive, private and sensitive information is collected and shared extensively with known or unknown entities, often without one's knowledge (Wei et al., 2014; Yun et al., 2019). This challenge can also be seen in the retail industry and services, where private data are collected through IoT devices to provide customers with a tailored experience.

In what follows, we explore previous research on the IoT applications in the service industry and smart stores and the challenges of IoT diffusion. Then, we examine the theoretical background of the IoT technology adoption and diffusion for service industries and smart stores to frame the research agenda for our field study.

2.1 IoT and Customer Journey in Smart Stores

The World Economic Forum identified IoT as one of the eight technologies expected to disrupt the retail industry in the near future (Accenture, 2017). In the potential store of the future, IoT-enabled environments are helping to feed the trend of moving from product-centric to an 'experiential' customer journey (Grewal et al., 2017). From a business perspective, the radical advantages that IoT can facilitate through real-time instrumentation, where the automation and optimisation of manual tasks can reap massive efficiency benefits, especially within industrial processes (Gierej, 2017). The simple reduction in hardware costs for an organisation's infrastructure and the generation and use of big data are considered the main drivers for investment in IoT. From an individual perspective, the value that IoT creates for a customer exists in its ability to predict and address customer needs in real-time. The ability for products to stay current and up to date without manual interaction, and the generation of meaningful data that can be used to enable personalised services support a 'path to profit' that is focused on the ability of the IoT to stimulate recurring revenues through a closer relationship with the customer (Metallo et al., 2018).

The services industry has been radically transformed due to the emergence of IoT applications. More specifically, in the retail industry, IoT is streamlining and automating processes that revolutionise services and the overall customer/shopping experience, introducing significant and simultaneous benefits both for consumers as well as businesses (Giebelhausen et al., 2014a). IoT-based technologies can provide personalised promotions to customers in order to manipulate their path through the store (Hui et al., 2013) and induce a rise in the value of the customer's basket. A different facet of personalised shopping demonstrates that encouraging shopping on a mobile phone reduces the need for blanket discounts, which overall reduce the company's costs (Wang et al., 2015). In other studies, the use of big data analytics to control in-store pricing showed that for a 100 stores enterprise, the increase in profits as opposed to human pricing control could be up to $11 million (Bradlow et al., 2017).

For firms adopting IoT, superior customer experience as well as supply chain optimisation and innovations in in-store experiences can be achieved through the technology, resulting in higher efficiency and profitability for the business (Gregory, 2014). Data from IoT sensors, such as environmental and motion data, enable retailers to offer personalised, tailored customer experiences by monitoring store traffic and customer demand in real-time; allocating assistants where most needed or adjusting the store layout; increasing store management efficiency in smart stores where the stock of products is being updated in real-time; and monitoring and predicting in-store waiting times. Although not linked to the IoT necessarily, sensor networks support the collection of 'big data', which in turn helps better explain an environment (whether physical or social). However, sensor-enabled solutions, such as smart shelves and robotic assistants can monitor a store's real-time performance, which constitute some of the most prominent examples of IoT applications in the retail industry, showcasing the unique nature of IoT applications in the services industry (Intel, 2017).

Technological changes and implementations in retail, such as IoT, have significantly influenced consumer decision making (Hamilton, Ferraro, Haws, & Mukhopadhyay, 2021). For consumers, the rapid diffusion of IoT in the retail sector has radically transformed customer experience and, more specifically, the customer journey (Hoyer et al., 2020) throughout all of its phases, from pre-purchase to purchase and post-transaction stage (Lemon & Verhoef, 2016). In the pre-purchase phase, aspects such as smart trolleys, smart mirrors and interactive changing rooms can transform the customer's experience, offering a more immersive and personalised approach (Ogunjimi et al., 2021; S. Shankar et al., 2021). New and innovative touchpoints have been introduced, while older ones have been re-developed to enrich customer experiences further and create new value (Hoyer et al., 2020). Customers can be identified the moment they enter the store through beacon technology and receive personalised notifications and recommendations through their smart devices, based on their purchase history as well as personal preferences. Aiming to revolutionise the transaction stage of the customer journey, retailers have been incorporating several in-store disruptive IoT touchpoints that can enhance customer convenience as well as increase satisfaction, for example, by decreasing or even eliminating customer queuing altogether. From scanning the products on their own (e.g., Zara's self-check-out) and paying via smartphone or a wearable device, the purchase stage of the customer journey now includes walking out of the store with no checkout process at all (e.g., Amazon Go) (Shankar et al., 2021).

Overall, it becomes apparent that the implementation of IoT in smart stores is radically transforming the customer experience, with various new touchpoints being created and others being reconfigured (Hoyer, Kroschke, Schmitt, Kraume, & Shankar, 2020). Such transformation may exert significant influence on other interrelated aspects and follow-on consumer experiences, interplaying in one's customer journey; from customer satisfaction, and service quality, to trust in a company, customer engagement and firm performance (Lemon & Verhoef, 2016). While existing evidence shows that IoT services in retail have a positive impact on customer satisfaction and experience (Ratna, 2020), research in this area is still in its infancy. Considering that the customer experience constitutes a multi-dimensional concept relating to "… cognitive, emotional, behavioral, sensorial, and social responses to a firm's offerings…" (Lemon & Verhoef, 2016, p. 74), it is imperative to examine and realise the profound impact of IoT throughout the whole spectrum of the customer journey and the dimensions of customer experience.

2.2 Challenges of the IoT Diffusion in the Retail Sector

IoT presents numerous opportunities in the organisational environment and has the potential to revolutionise the way multiple industries operate. However, challenges in securing, verifying, and storing that data also exist, and these challenges act as a barrier to more widespread adoption and diffusion. Some of these challenges are prevalent for the IoT in general within a customer-facing industry. Nevertheless, the added dimension of the personal nature of the collected data has further security ramifications.

Firstly, with regards to data management and the vast amounts of data, an issue that arises pertains to how data is stored. Then, other questions pertaining to how 'quality' data is identified, isolated and prioritised also arise (Lazer et al., 2014a). Secondly, there is the issue of the mixed-media format of the data that is being transmitted and analysed and the infrastructural complications stemming from these processes. Within the hyper-connected and hyper-accelerated innovation cycle that exists within the technology sphere, there is potential for the advancements to become chaotic, especially without the concrete and universal regulations in place (Weber & Studer, 2016a). The issue of security can also be raised at the device level, which is intrinsically linked to the most critical issue of data privacy (Palattella et al., 2016a).

Several key factors create a bespoke challenge for IoT security and privacy: heterogeneity of devices, heterogeneity of data, and low power nature of devices (Al-Fuqaha et al., 2015; Atzori et al., 2010; Gubbi et al., 2013). These factors, combined with the increased number of devices within an IoT network, mean that security is paramount for the successful dissemination of the IoT.

Specifically, in the data driven IoT environment of the smart store, the customer journey is based on insight and personal information of each customer for a tailored shopping experience (Hu, Hu, & Cao, 2018). Services are based on the information shared through the IoT platforms where in a fully smart environment, the customer has to provide consent to divulge certain information to companies, and deny access to others (Brous, Janssen, & Herder, 2020). In the grand vision of the IoT, where all devices are interconnected, data control systems must be able to accurately control what data can be transmitted and to whom (Brous et al., 2020).

There are specific challenges that the IoT faces with regards to privacy. IoT use is not yet regulated as much as needed to ensure privacy and security for customers (Hu et al., 2018). Due to the heterogeneous nature of the IoT, the issue needs to be addressed from different perspectives (Hu et al., 2018; Lu, Papagiannidis, & Alamanos, 2018).

A study about consumer facing retail technology found that customers were highly supportive of a technology that reduced queuing times and yet were uncomfortable with proximity marketing (Inman & Nikolova, 2017). This indicates that it is a cultural shift towards accepting ‘help’ from technology that will help the adoption of ‘privacy-invasive’ technologies. This can be aided, as discussed above, by companies making a concerted effort to show that customer privacy is a priority.

Whilst the literature reviewed within this section pertaining to IoT privacy and security at a generic concept level comes from an abundant bank of research (Al-Fuqaha, Guizani, Mohammadi, Aledhari, & Ayyash, 2015), there is still more ground to be covered in the field of IoT adoption and diffusion with regards to data sharing and security challenges (Brous et al., 2020; Hwang, Kim, & Rho, 2015; Pauget & Dammak, 2019) Our study focuses on this gap and highlights the importance of IoT security and privacy in the customer-facing environment of the smart stores.

2.3 Theoretical Background

The present study seeks to address the gap in existing knowledge regarding the drivers and challenges associated with the implementation of IoT and offer potential solutions, emphasising a customer-facing service environment and smart stores within the retail sector. Therefore, the theoretical framing of this study draws from three streams of theory: the Diffusion of Innovations (to provide specifics for the diffusion of IoT as a technological innovation), IoT network background (to account for the IoT-specific aspects) and the service-dominant logic (to explore the specifics of service systems and the diffusion of IoT in smart stores - retail services).

There has been a scarcity of research on the secure implementation of an IoT system in a real-world environment (Metallo et al., 2018), considering security features within a retail environment. Seminal studies provide instruction on what to consider when setting up an IoT system; however, they do not cover all the challenges an IoT implementation may introduce (Goad et al., 2020). With security in mind, the framework for Industrial IoT (Boyes et al., 2018) can be used in the planning phase to ensure there are no intrinsic system flaws. While the framework provides valuable questions for considering the attack surface of an IoT system, practical solutions are not supplied.

In order to understand how new technology disseminates throughout society, the Diffusion of Innovations or DOI as it is abbreviated (Rogers, 2003) presents a useful conceptual framing. The DOI framework presents the requirement to understand how a new application technology (in this case, the IoT in a customer-facing environment) can be evaluated in terms of successful proliferation and the consequent challenges that might be faced during implementation. The Diffusion of Innovations theory presents five variables that determine the adoption rate of innovations: Perceived Attributes of Innovations, Type of Innovation-Decision, Communication Channels, Nature of the Social System and Extent of Change Agent's Promotion Efforts. While all the five variables provide a rounded view of how likely technology is to flourish within an industry, the perceived attributes of innovations are the most widely considered in the literature (Rogers, 2003) and adopted in this study.

Historically, the service industry has focused on exchanging goods, resulting in a landscape that is aligned towards a transactional infrastructure, facilitating the exchange of tangible resources (Lusch and Vargo, 2006). However, this landscape has changed in recent times to include intangible assets, the co-creation of value, and relationships. This has resulted in the development of the Service-Dominant (SD) Logic (Vargo and Lusch, 2008) which is encapsulated in the shift occurring within the services industry and is especially prevalent in retail and customer-centric studies (Grewal et al., 2017). Based on the SD logic, there is a perspective on service innovation (Lusch and Nambisan, 2015), segmenting the concept into three key themes: (1) Service Ecosystem - the network of actors that governs the landscape of the service exchange, (2) Service Platform - the combination of resources (both physical and intangible) that form a provision, (3) Value Co-creation - the actions that motivate the resource integration and actor interactions within the service ecosystem. The SD logic departs from other logics in-service science by heightening the value creation process, broadening the scope of resources, and supporting collaboration within and between service systems.

Combining the work of Lusch and Nambisan (2015), Rogers (2003), and Boyes et al. (2018) allows us to formulate the theoretical framing for our field study. Specifically, we draw from Boyes et al. (2018) in order to identify the IoT network vulnerability aspects, whereas the S-D themes (Lusch and Nambisan, 2015) and the perceived attributes of innovations (Rogers, 2003) inform the holistic appraisal of the cyber-business environment. The decision to ground the research in a deductive design with a specific amalgamation of theoretical background reflects the pragmatist standpoint of this study into the IoT within a Retail Industry environment. For a genuinely holistic appraisal, it is not sufficient to merely consider the technical aspects of security design without an appreciation of how the technology interacts within its environment to generate value and consider the factors that will impact implementation and reception.

3 Research Design

The research study is a contribution to the field of evidence-based management through the critical evaluation of relevant, high-quality research and practitioner expertise and judgement (Denyer and Tranfield, 2006; Tranfield et al., 2003). Therefore, the study is multifaceted, taking evidence from existing academic research and harnessing the explicit and tacit knowledge of those who work within the field (Bryman and Bell, 2011). The approach falls under the definition of an elicitation study as described by Edgar and Manz (2017) with an exploratory qualitative field research design.

Random sampling is not appropriate in an elicitation study, where the objective is to capture knowledge from experts (Marshall, 1996; Suri, 2011). Instead, a purposeful key informant sampling technique is required (Marshall, 1996; Suri, 2011). We thus aimed at identifying industry professionals who work within a retail environment and in an area with an IoT focus. We were also open to snowball sampling, whereby respondents were asked to suggest other professionals from their own networks who could provide interesting insights (Marshall, 1996; Suri, 2011). In total, ten people were interviewed, each of them providing an information-rich case where the experience was the critical sampling focus. Each participant shared their expertise and experience in multiple organisations where they have worked with IoT over the previous years. A description of our respondents is displayed in Table 1.

Table 1. Description of Respondents

ID	Industry	Main Country of Operation	Global
1	IoT Consultancy	United Kingdom	Yes
2	Retail	United Kingdom	Yes
3	IoT Services	United Kingdom	No
4	IoT Consultancy	United Kingdom	Yes
5	IoT Consultancy	United Kingdom	No
6	Retail	United Kingdom	Yes
7	Hospitality/ Retail	United Kingdom	Yes
8	Hospitality/ Retail	United Kingdom	Yes
9	Hospitality/ Retail	United Kingdom	Yes
10	Retail	United States (with operations in the United Kingdom)	Yes

The individuals selected for the field study represented the views of different retail organisations in the UK or consultancy for IoT implementation (10 organisations/consulting firms in total), where the "experience in IoT for retail customer-facing applications" was the primary selection criterion. Each participant was interviewed twice (appx. 30 minutes interviews) a) for the exploratory interview stage and b) at a follow-up confirmatory stage (once the themes were generated).

For the purposes of data collection, we conducted semi-structured interviews. We developed an interview protocol on the basis of our theoretical framing, which we shared with our respondents pre-interview as a quality measure to facilitate full responses (Patton, 2002). This approach was chosen as opposed to an 'informal conversation' or 'standardised' method because it provides a better opportunity for detailed answers on the specifics of the respondent's knowledge. Equally, as the study's objective was not to compare the knowledge of professionals, rather consolidate it, there was arguably a call to increase variance rather than reduce it (Marshall, 1996; Patton, 2002). Given our pragmatist approach, care was given to ensure that and identify problems; respondents were encouraged to provide potential solutions for the factors they highlighted without leading them.

The interview guide was designed to reflect the multifaceted nature of IoT applications in a customer-facing environment, one of smart stores. Starting with more high-level questions, which address how and why the IoT is used in industry (and specifically in a customer-facing service environment), the guide then examines the specific setup within each organisation and how each participant considers IoT diffusion and the implications for the customers. This is then placed under a pragmatic project management lens, both in the context of real-world experience and in a hypothetical scenario where 'best practice' can be observed. The interview guide was used as a basis for the conversation, but as explained previously, due to the semi-structured approach taken within this research, it was not always strictly adhered to. Instead, the guide was primarily used as a springboard for further probing, whereby the interviews were allowed to flow in the direction of the interviewee's expertise but guided by the themes explored by our research.

For data analysis purposes, we adopted a thematic analysis to identify the thematic clusters that emerge from our interviews and capture opportunities and challenges. Braun and Clarke (2006) describe thematic analysis as "*a method for identifying, analysing, and reporting patterns (themes) within [qualitative] data*." Theme development was done via a hybrid inductive/deductive approach which facilitated finding general conclusions from the full dataset (inductive) whilst ensuring the more specific research objectives were also explored (deductive) (Boyatzis, 1998; Braun and Clarke, 2006). Specifically, we analysed the interviews in order to identify the major themes emerging from the data. This identified business considerations, devices and infrastructure, project management, privacy and data, and human in the loop as the major themes that organisations face when implementing the IoT in-store. During the second phase, we examined these themes in more detail by iteratively reading through them, comparing them and rechecking the consistency of our coding with the aim to classify and organise our sub-themes across the interviews. This resulted in sixteen subthemes, organised along with the five major themes, lending themselves to the security aspects of specifically implementing IoT systems within a store. Finally, the reliability analysis entailed summarising our findings, evaluating our findings, identifying relevant and representative vignettes from the interviews to illustrate the emerging themes, and relating our findings to the existing literature. Table 2 encapsulates the findings of our analysis.

Hennink, Kaiser and Marconi (2017) describe code saturation as the stage where no additional issues are identified, through an inductive, content-driven approach, as raised by respondents. To ensure code saturation, as we were conducting the interviews, we were continuously analysing our material to establish that no more themes were emerging. We thus stopped conducting additional interviews when we reached code saturation.

Table 2. Data Coding Structure

Themes	Subthemes	Codes
Business Considerations	Drivers	• Customer expectations • Being in the market and remaining competitive • Improves the 'customer journey' • Cost-effective, with better insights (market research can be cheaper)
	Challenges	• Heterogeneous devices (standards) • Security (cost, oversight of devices' production) • Affordability and operational costs • Security costs have to balance in favour of business profits
	Opportunities	• Personalised service to build brand loyalty (personalised customer journey): footfall cameras, wireless tracking, feedback, how people move within a store) • Align with 'fail fast' organisation mentality • USP for the first UK store to 'crack IoT' (if 'done well')
Devices and Infrastructure	Security (by) Design	• Device/Systems provenance (manufactured by 3rd parties) • Diverse/changing regulations and data handling • Patching
	Device management	• 'Shadow IT' • Network access control (monitoring what's on the network) • Restrict access of IoT devices to networks • No access to the corporate network
	Heterogeneity and Complexity	• No standardisation • Operating costs increase • Identification of 'experts' in multiple OS/devices • Response time and protocols

		• Training
Project Management	Implementation	• Business case for the project – is there ROI? • Project design (including ill-suited infrastructure for an IoT capable store - retrofitting) • Procurement • In-house Device testing (taking devices apart to see how they work) • Trialling: no trial equals 'firefighting', not just for security, but for usability, too, trial in the busiest store • Design of services: involve security team at all stages, needs a business case and ROI • Roll out and monitoring
	Security Lifecycle	• Ensure is considered from day 1 (continuous monitoring) • Consideration for procurement and running costs
	Organisational Culture	• Impacts on privacy-related perceptions • Continuous observation for identifying potential concerns • Change management and resistance to change
Privacy and Data	Compliance	• Access, rights and permissions • Covered against GDPR • Data storage: how long for, where, how • How can customers access their data (if they request to)
	Understanding Data	• Not all data is needed (collect only that which is needed) – cherry pick what to process and store • Where does data come from (is regulation the same everywhere?) • Value of data (individual and combined data streams) - Metadata can be used to create 'real' data • Infrastructure
	Responsibility	• Outsourcing doesn't absolve a company from protecting customer data • Show customers, you are serious about data handling (customer requests) • Being GDPR compliant and customers being 'comfortable' with data collection is different.
	Supply Chain	• Need to be confident that a supplier has at least the same security controls as you around customers' data • Hardware device manufactures may not be concerned about data protection • Personally, identifiable information is the lifeblood of the organisation • Retailers are more concerned with aggregate data
Human in the Loop	Usability Vs. Security	• Security shouldn't interfere with the employee's role • Security should be balanced (allow employee innovation) • Use the same processes as much as possible
	Education	• Educated on 'security device.' • Protect against human errors (but educate the human, too)
	Behaviour	• Employees will find loopholes to make things work 'like they used to.' • Recommendations are unclear so hard to pass on to employees • Tie education piece to the employee experience/ day to day activities (make it relatable)

4 Findings

We present our findings organised along with the five main themes that emerged through our empirical material: business considerations, devices and infrastructure, project management, privacy and data, and human in the loop. A summary of our findings is illustrated in Figure 1.

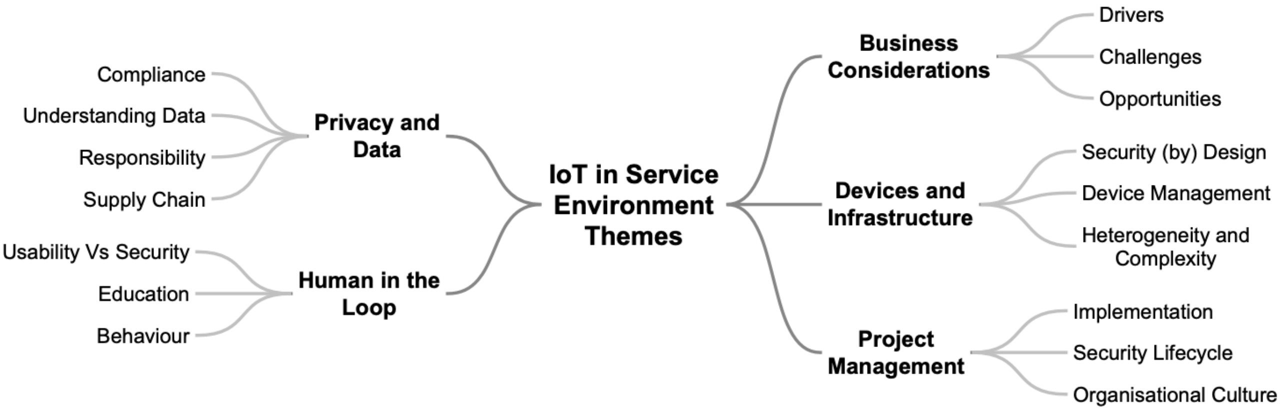

Figure 1. Themes and Sub-themes arising from the interview data

4.1 Business Considerations

Business considerations emerged as a core theme, whereby our respondents identified the 'greatest business drivers', the 'key challenges', as well as the opportunities for implementing an IoT system within a customer-facing service environment. Customer expectations emerged as a driver for adopting IoT as businesses need to appear as keeping up with the pace of technology. Therefore, businesses might feel pressured to introduce IoT so as not to be left behind:

"There's a fantastic opportunity for the first UK high-street retailer who does it and does it well- a massive opportunity for them commercially to use it as a USP. You should be on the front of that [the IoT] and driving it. You shouldn't be a follower; you should be a trendsetter, a champion who spearheads it through." (Respondent 7)

However, the salient part in the above statement is the call for the use of IoT to be 'done well' in a retail environment to the extent that it can be considered the USP of a brand. While the IoT is being used increasingly in the services industry, a business has made itself synonymous with IoT, at least in the UK context.

The respondents also identified the potential from the amounts of personal data gathered by connected devices towards developing personalised customer journeys through a store. However, they also took a higher-level approach noting how IoT devices, generally being smaller and cheaper, enable an organisation to exact fast change in a cost-effective way:

"They [the IoT] are a concept of a device which fits very neatly with a lot of the paradigms that organisations tend to go for nowadays: 'run fast and fail quickly' for better or for worse…" (Respondent 8)

Challenges were also diverse, possibly due to the different specialisms of the respondents. However, they mostly focused on the heterogeneous nature of IoT devices:

"Most of the IoT stuff is the different spec. There are no standards to follow, so each of the devices is built on a different base, and having a baseline for the infrastructure is difficult because it cannot be defined." (Respondent 1)

Further probing revealed the criticality of balancing security, costs and benefits, and tackling some of the key challenges of IoT implementation:

"You have to weigh up the pragmatic bit of what it will deliver for your business against what security controls you need... The controls you put on it [a device] need to be proportionate to the stuff you are trying to protect." (Respondent 9)

Along these lines, several respondents (Respondents 3, 6, 7 and 9) indicated that, because security is an operational cost rather than a revenue stream, businesses need to be cautious in not overspending for security (i.e., "not spending £5 million on a £1 million problem" Respondent 9). This highlights that security for IoT-enabled stores and spaces is an ongoing cost, which businesses will need to budget for on a continuous basis; as such, it has to be proportional to what they are protecting (e.g., central corporate systems vs point-of-sales), so as not to overspend.

4.2 Devices and Infrastructure

Security is considered both at the level of the individual device as well as at the level of the network. With regards to the security features of a device, provenance is of particular concern, especially in relation to different regulations around data handling. For example, one respondent (Respondent 9) observed how the geopolitical environment could create obstacles for security. They noted that, since the US ban, for example, on Huawei, its tablets are no longer on the Microsoft list of enterprise devices. The implication is that companies can no longer patch and maintain Microsoft applications on Huawei devices and are thus potentially vulnerable to being attacked; in other words, companies can no longer use these tablets in a secure way for IoT service environments.

Given the low cost and easy-to-use nature of many IoT devices, many employees feel empowered to introduce devices onto the store network. A key challenge is keeping track of the many different devices on the network, and especially in relation to 'shadow IT' (Respondent 2), i.e., the technology used within an organisation but approved explicitly by the IT function. Respondent 7 expanded on this and discussed that the organisational structure exacerbates this risk because, for projects that are not considered big enough to involve IT, the security function tends to be bypassed. Given the accessibility of IoT devices, this increases the opportunities for using shadow IT and amplifies its negative impacts.

With regards to practical advice around the implementation of IoT within the store, the message that emerged was that of consistency (e.g., *"try and have some consistency"* (Respondent 8)). Given the security challenges introduced by a heterogeneous environment, this idea is based on the premise of *"simplifying the problem, so your control remit is simple"* (Respondent 5). Simplicity and homogeneity suggest that there are some advantages:

- Tracking of devices;
- Monitoring of threats and alerts for particular systems;
- Easier training;
- Identification of expert for all devices;

- Faster response in a crisis with all devices following the same protocol;
- Reduced operating costs.

Whilst it does potentially give commonality to a vulnerability, on balance, securing one thing well seems more viable than successfully protecting and monitoring multiple systems.

4.3 Project Management

The management of the implementation of an IoT system within a customer-facing service environment emerged as one of the important themes. Table 3 provides the amalgamation of the suggested steps, from concept through to rollout.

Table 3. Suggested steps for managing the implementation of IoT systems

Step	Respondent	Detail
Business Case	1,3,4,7,8,9	Why choose an IoT solution? What data will be collected? What business advantage will be gained? What is the effect on staff/ customers? What is the budget/ how much will it cost?
Project Design	3,5,7,8	Do you need to hire anyone to ensure you have the right knowledge? What's the project environment? Can you make changes to the building? Does the solution meet business requirements? Does the solution meet security requirements? Does the solution satisfy internal compliance?
Procurement	All	Soft market research on the best provider. What is the in-built security of the devices? Does the vendor sufficiently protect data? Is the vendor lawful and ethical?
In-House Device Test	3,6	Take the device apart to see exactly how it works- does it function as promised?
Closed Trial	7,8	If possible, test in a mock environment- can show if it will interfere with existing processes without losing revenue.
Real Trial	All	Trial in a variety of different types of store. Are there any security flaws? Are there any usability flaws? Iteratively optimise the system. Does it meet the business case?
Service Design	3,6,7,9	Who is responsible for maintenance of the devices: for both functionally and security? What does that involve? What are the running costs?
Roll-Out	All	Batch approach. Suggested to start rollout near to locations that can easily be accessed by maintenance.
Life-Cycle Monitoring	3,5,7,8,9	Functional delivery of 'Service Design.' Periodically assess against business case- is it meeting objectives?

Regarding the security, it is important to think about it from the first of the project, as retroactively fitting on top of systems typically incurs higher costs than building it in during the process (Respondent 5). It is also needed that:

“there is at least a partial InfoSec input at each stage, some are just a chat, and some are far more in-depth. But if you get it at every single stage of the way, that’s how you get your end-to-end assurance.” (Respondent 8)

However, security is a dynamic concept:

“The security posture of a device is never static. Things change; people are always looking for ways around things. It might be secure on day one, but it might not be secure down the line.” (Respondent 3)

This perhaps presents more of a challenge for IoT devices than other technologies because many IoT devices do not have a direct user interface. It is not always obvious (e.g., through alerts) when a device needs to be updated or its license if its license is about to expire. Business and security requirements will need to be constantly monitored and assessed (Project Design). Such potential changes will need to be reflected in the Procurement costs and the Service Design (running costs).

Another approach to project management issues was raised by Respondent 9, who commented that:

“Issues-wise it tends not to be with technology; they are more regulatory- so HR: people’s ability to adopt change.”

Although common to all forms of organisational change, many IoT implementations exhibit an observational nature. Organisations may likely face complaints from employees regarding privacy infringements, whereby the workplace becomes a “Big Brother State” (Respondent 9). The implication for the IoT project is that it is likely its implementation will be received with scepticism and resistance from the employees, which in the longer term may have negative consequences for the project in general.

4.4 Privacy and Data

When discussing the challenges of implementing IoT solutions, our respondents considered data and privacy almost synonymous with the IoT. One could argue that data and privacy are more universal concerns, extending beyond the area of IoT (e.g., for online social networking applications, such as Facebook). However, the attitude of many of the respondents towards GDPR was that of assurance that their organisation would be compliant. However, there was also a concern that organisations do not always fully understand or know what data they capture, both in terms of volume and content.

With the IoT’s capacity to monitor an environment with higher granularity than before, it is not so much the individual data streams that cause an issue so much as the collective context of the information:

“Supposedly anonymised metadata can be so detailed that it can easily be used to identify you.” (Respondent 5)

By not understanding the power of combined data, organisations fail to put sufficient protection around it. However, cybercrimes are not new crimes and are not always facilitated by state-of-the-art technology. It is the crossover of the two, which is new. It is that which makes the versatility and omnipresence of the IoT more of a challenge: it introduces an exponential increase of threat vectors that can be combined:

"The IoT is reasonably new… It always takes people's skills and experiences to develop controls to catch up… When you mix a niche technology area with a fast-growing new concept, they catalyse each other in terms of risk. You don't know what to look out for, and you don't know how to secure it even if you did!" (Respondent 8)

With regards to the implications in the store, privacy is subject to the practical bandwidth limitations of the businesses and their processes. For example, Respondent 10 commented that:

"We [the company] *try and make sure that only relevant data is taken from systems- we cherry-pick what is useful and send that to the cloud."*

This is particularly salient when, as pointed out by Respondent 7, one considers the store environment where bandwidth is limited and has to be shared with point of sale devices that are critical for business operations. It is also relevant for the scenario where a personalisation service is available in the store, but a customer decides to disable the function, and the request to cease data collection and notifications needs to be processed quickly in order to respect that the customer's right to privacy.

Another issue relates to the concept of data security in the supply chain. Within a service environment, there may be a disparity between the priorities of data protection for service providers, where the organisation *"would be very careful with the customer's personally identifiable information as it's their lifeblood" (Respondent 5)*, and the hardware device manufacturers, where data protection is less of a priority. Respondent 5 further added that:

"You need to know that a third party has the same or better security controls than you would have over that data, because, whilst you are outsourcing the processing of that data, you are not outsourcing the responsibility for it." and because of this, it is critical to have the right of audit over the supply chain.

4.5 Human in the Loop

The most typically discussed topic was that of usability versus security:

"There's the old InfoSec joke that the most secure computer is the one that's turned off- but that's no use to anyone!" (Respondent 8)

Respondent 9 shared anecdotal evidence from a large retailer who had changed its policy from allowing no personal devices on the shop floor to equipping all employees carrying with a mobile device for looking up products and informing customers where they can be located. The strategy is based on the premise that:

"Security has to be very balanced. If you make something so controlled that someone can't use it - they won't! They will do something completely different. And the way the world is today, there will always be a different way of doing something." (Respondent 9)

In effect, while the retailer may not have as much control over security, they can be confident that all employees use at least the same process, thereby limiting the unknown variables, which then makes it easier to place controls around.

As Respondent 3 observed when talking about the 'human in the loop':

"It's an interesting debate, and there are many things about whether you try and protect against the human, or you try and educate the human… we try and do both."

Along these lines, all respondents discussed that education around security should develop around generic good practices, with some more practical suggestions: make the message clear and succinct; relate it to the function of the employee; use multiple sources to engage.

5 Discussion

5.1 Synthesis of the results with the existing literature

This study aimed to better understand the drivers and challenges of IoT implementation within the retail industry, particularly within the smart store space, following the SD logic and the diffusion of innovations approach. Our analysis shows that, when it comes to the implementation of the IoT within the store, five critical aspects have to be considered: business considerations, devices and infrastructures, project management, privacy and data, and keeping the human in the loop. This section integrates and discusses our findings in relation to the existing relevant literature and further discusses the security-related implications for each of these five themes.

5.1.1 Balancing drivers and challenges

The power of IoT in generating unprecedented insights into customer behaviour is widely reported as a driver in the literature (Gregory, 2014; Lee and Lee, 2015; Metallo et al., 2018). Similarly, the ability to increase the efficiency of processes through the automation of menial tasks is also commonly acknowledged. For the service sector, in particular, there is a trend towards personalisation and experience-driven sales (Accenture, 2017; Balaji and Roy, 2017; Gregory, 2014; Grewal et al., 2017) because these are expected by customers (Priporas et al., 2017).

However, in our study we find that responding to competitive forces is likely a stronger argument in favour of implementing IoT in physical stores. In more detail, while retailers suggest that they do experience pressure to leverage IoT for satisfying customer expectations, more often than not, they perceive IoT-enabled solutions to be critical towards achieving and retaining their competitive advantage. At the same time, our study shows that IoT-based systems support businesses in improving the customer journey because they support personalisation and offer insights, the latter often being better and more affordable that competing market research solutions.

Yet, investing in technology is not as straightforward and choosing to invest in IoT because one’s competitors are doing the same, can result in more challenges than opportunities. The heterogeneity of devices is widely considered the key obstacle for businesses wishing to implement an IoT solution (Lee and Lee, 2015; Sicari et al., 2015) as this entails additional complexity with implications for security and interoperability. Specifically, heterogeneous IoT devices, while monitoring the environment and producing data streams in multiple formats (such as video, sound, and metrics), they result in a vast quantity of diverse data, with each format requiring a different transmission and storage infrastructure to be considered ‘secure’ (Roman et al., 2011). In terms of the information being used for analytics, having such a large pool of data introduces a great challenges for data storage and data relevance (Sun et al., 2016). This ties back to the adage of ‘bigger data are not necessarily better data’(Lazer et al., 2014) which supports the process of pre-filtering ‘useful’ data. Our findings indicate that this further lends gravitas to the issue of the bandwidth ceiling within a store environment and emphasises the importance of knowing what data is being generated in order to manage it effectively.

In addition, heterogeneity of devices relates to the security of IoT systems by default. We find that security within the retail sector needs to be proportional to what it is protecting, i.e., decision makers need to consider what is the minimum security expenditure that can satisfy the retailer's risk appetite. Proportionality allows the business to make reasonable expenditures which in turn allow the business to maintain normal operations. The implications emerging from multiple heterogenous devices in relation to security costs have been discussed in earlier studies (Gierej, 2017; Zhao and Ge, 2013), without however referring to proportionality. This may be due to that existing IoT studies are not typically multidisciplinary and they either adopt a business approach (e.g., Metallo et al., 2018) or a security-focused approach (e.g., Ning et al., 2013). As such, the business side approaches security as something that needs to be addressed but not necessarily rigorously, whilst security research is focussed on best practices, unencumbered by practicalities.

When considering the costs, Yee (2004) notes the importance of specificity in parameterising system requirements and capabilities. This, he explains, facilitates more accurate security cost projections because specificity supports demarcating the necessary spending on different types of systems to make them secure on the basis of their criticality for the business (in terms of function or data). This observation, whilst made before the IoT became popular, our findings illustrate that it remains pertinent for ensuring the financial viability of security.

5.1.2 Security of heterogeneous devices and homogeneity

With regards to *devices and infrastructure*, our findings show that having little to no control over the in-built security of devices manufactured by a third party can be problematic. On the one hand, this refers back to the issues arising due to the heterogeneity and complexity of devices and infrastructures. On the other hand, it also refers to standardisation and the lack thereof. The lack of standardisation suggests increased operational costs because it requires the involvement of several different experts, either in relation to training or in relation to recruitment, who will need to manage and monitor the numerous but heterogeneous devices and systems.

At the moment, various governments have identified that third-party manufacturing and the lack of standardisation on security are indeed critical. For example, the UK government released in 2019 a list of 13 'secure by design' features that all IoT devices should abide by in order to give a minimum level of security (ETSI, 2019). In addition, the US National Institute of Standards and Technology released two reports, addressing IoT device manufacturers (Fagan et al., 2019a), and businesses and organisations that use IoT (Boeckl et al., 2019).

Our findings suggest that homogenising the device environment wherever possible can reduce the security challenge and provide intuitive customer-facing services. Yet, to date, homogenisation of the device environment does not appear prominently in the security literature. Boeckl et al. (2019) suggest that devices of the same manufacturer are easier to manage and monitor centrally, whereas devices of different manufacturers introduce vulnerabilities in the IoT lifecycle and require diversified management of updates and alerts. The latter leads to further complications whereby integrating a wide range of devices within a single information security policy may result in overload and uncertainty, resulting in policies not being always adhered to. For this reason, standardisation is said to reduce the need for a diversified security policy (D'Arcy et al., 2014). However, our findings illustrate that ultimately it is a business decision as to whether "having all your eggs in one basket" and improved manageability results in an acceptable trade-off. On this basis, appreciating which baseline security features 'should' be included in an IoT system is critical for procurement decisions.

5.1.3 Managing the IoT implementation

Our study shows that *the management of an IoT project*, influences its implementation, the security lifecycle, and the organisational culture. Implementation of the IoT infrastructure in the store space should always start with a business case, like typical information system projects, and consider the customer journey. This approach allows developing common understanding with regards to the IoT system and the Return on Investment (ROI). Specifically, Palattella et al. (2016) explain that, in IoT, there three main areas with high ROI, namely efficiency savings, big data, which is often considered the main investment motivation due to the superior customer insights, and infrastructure costs, because IoT alleviates the costs pertaining to (re)wiring the store space.

In addition, our findings illustrate that the differences between IoT and 'traditional' IT (i.e., modes of interaction with the physical world, access, storage, and monitoring, security and privacy, and functionality) (Boeckl et al., 2019) require close consideration during the entire lifecycle of an IoT project (technical and service design, procurement, implementation and monitoring). Along these lines, Fagan et al. (2019) offer some recommendations, which we consider relevant to IoT projects in the retail sector, particularly when considering procurement:

1) What are the security features of the device?
2) What exactly does the device do, and what mechanisms does it use to facilitate that?
3) How are software and firmware updates delivered?
4) When does the device stop receiving product support?
5) How should the device be handled at the end of life?

However, our study shows that security considerations need to extend beyond procurement costs or confined within the project lifecycle. Instead, security should be approached as an ongoing running cost, and one that is considered together and iteratively with usability and the customer journey so as to reduce potential conflicts between the two, and avoid future spiralling costs. Having said this, the idea of making a system both more secure and more efficient is often considered a *'Unicorn State'* in InfoSec (Respondent 8).

With regards to organisational culture, our findings illustrate that the introduction of IoT systems often results in changes in everyday workflows and employees' roles. Earlier studies have explored the role of the employee in relation to IT-induced transformation in the service sector while drawing attention to how technology may either 'augment' the capabilities of employees or replace them altogether with the view to remove inherent human performance variability (Larivière et al., 2017; Pavlou, 2018). However, this is not confirmed by our study. On the one hand, our findings suggest that there is a need for employees to be ready for change in order to successfully engage with a changing role, and this necessitates the availability of training opportunities, raising awareness and developing change management programmes (Larivière et al., 2017). On the other hand, our findings show that the greatest concern seems to be employees' perceptions with regards to their privacy, which can influence negatively organisational culture. In addition, one could argue that uncertainty and potential negative perceptions with regards to one's privacy in their workplace may create risks for the organisation's security: our study does not offer direct evidence about this, yet existing literature showcases that disgruntled employees often pose an insider threat to an organisation's security (Greitzer et al., 2012).

5.1.4 Privacy concerns and the customer journey experience

To date, concerns regarding *data privacy and trust* have been hindering the widespread adoption and diffusion of the IoT (Palattella et al., 2016). These concerns have also been expressed in our study, however from a different perspective. Our participants consider complying with GDPR as being the default position, which nevertheless creates considerable challenges with respect to handling data and specifically personal identifying information (PII). They consider that their organisations are able to function responsibly throughout the entire process of collecting, storing and processing PII, despite the involvement of third parties whose practices cannot always be controlled for. This suggests their deep knowledge and understanding of the nature of data along the entire supply chain.

Interestingly enough, our participants further highlighted that their customers would happily provide their personal information if they were to receive something in return, such as personalised services. However, customers may likely have little understanding of what such personalisation requires as well as what parting from their PII may entail (Walker, 2016). For example, personalised services, such as targeted advertising, may be perceived as too intrusive and not well-received (Inman and Nikolova, 2017a). Such negative perceptions may be exacerbated by practicalities, such as bandwidth limitations within a store environment. In the hypothetical scenario of a customer opting out of personalised notifications as they move through the store, low bandwidth may result in delays in processing their request. In this case the customer may interpret such delays as if their request is ignored, and that their privacy is in jeopardy. Naturally, this will have negative implications for the customer journey. In addition, such delays may potentially be non-compliant with GDPR and, on the basis of our findings, they indicate low levels of responsibility regarding data and request handling. As a result, deep knowledge and understanding of PPI is crucial, and this extends to metadata as well. Specifically, our findings reflect the risks regarding privacy breach when metadata can be pieced together despite previously applied anonymisation techniques. A recent report by the National Institute of Standards and Technology (NIST) addresses this issue by recommending continuous mapping of PPI data through a system in an effort to mitigate deanonymisation via data aggregation (Boeckl et al., 2019).

5.1.5 Usability and security of IoT in a customer-facing environment

Our study highlights that maintaining the human in the loop relates to achieving a balance between security and usability, cultivating useful behaviours and training. We find that security protocols often restrict store employees and reduce their opportunities to innovate while serving customers. To combat this, our participants indicate that training and particularly security-focused training is important, but it can be beneficial only when explicitly relevant to the employee experience, and specific to the devices employees typically use as part of their workflow.

While this balance between security and usability has been addressed by earlier studies (e.g., Ben-Asher et al., 2009; Yee, 2004), little to no attention has been paid to the IoT context thus far. In the IoT context, our findings show that this technology introduces further opportunities to circumvent security protocols. We also find that security needs to be designed with human behaviour in mind to address potential usability shortcomings. Previous studies have found that when usability is low, users are inclined to 'bend the rules' and enact workarounds (e.g., Zamani et al., 2019), and such behaviour is relevant to the IoT context, too. In many cases, introducing an IoT infrastructure will result in increased complexity with respect to the technological environment and will introduce intricacies in employees' workflows. Studies have shown that in such cases, increased security requirements may result in Security Related

Stress (SRS) which has been associated to moral disengagement and security policy violations (D'Arcy et al., 2014). It could equally be argued that the IoT can streamline processes, and therefore reduce rather than increase complexity, with front line employees needing to abide with fewer security protocols and reduced SRS. In all cases, however, it is more often than not that employees will be able to find ways to work around the system (Alter, 2014), and security protocols will be bypassed.

5.2 Implications for Theory

Our field study provides a content-rich understanding with regards to the specific drivers and challenges for IoT adoption and diffusion in smart stores. It also provides an enhanced understanding of the initial theoretical aspects, further specifying IoT technology in store. Discussions with our participants were focused around our initial research question: "What are the drivers and challenges that companies face during the implementation of IoT in smart stores and which of them are relevant to the customer-facing services?". Therefore, the major contributions of our study are positioned within the security and privacy domain, whereby these are major concerns for customers and retail stakeholders, and a challenge for the successful IoT diffusion. Specifically, we find that privacy and security can jeopardise the customer journey, and create negative implications for customers' buying behaviour and challenges for the smart stores where the IoT is implemented.

The second contribution of this study is that it extends prior research on customer experience and satisfaction from an Information Technology perspective. Specifically, while prior work has focused on smart customer experience in the retail domain, primarily from a consumer perspective (e.g., Roey et al., 2017), our study extends current understanding with regards to IoT in particular, while considering the challenges for both customers and retailers. This is of particular significance because the technology of IoT comes with specific opportunities and challenges. On the one hand, the opportunities and challenges of IoT are distinct from those of other technologies, such as the Blockchain. On the other hand, to date and to the authors' knowledge, the literature pertaining to customer satisfaction has not yet identified how these may influence consumers but also the implications for retailers who seek to offer unique customer journeys.

In addition, because our study focused on the IoT devices in store as our unit of analysis with the view to explore customer perceptions, we adopted the principles espoused by retail scholars to identify the specifics of the customer experience (Homburg et al., 2017). Namely, in conceptualizing our study, we adopt the innovation perspective, which is often applied in studies on smart store technologies (Pantano & Viassone, 2014). Namely, in our study we adopt the conceptual lens of the Diffusion of Innovations Theory (Rogers, 2003), which determines the rate of adoption of innovations. To date, technology adoption theories, such as the Unified Theory of Acceptance and Use of Technology (Venkatesh et al., 2003) and the Diffusion of Innovations Theory are often used for in theoretically framing studies in the area of smart retail technology, with the view to compare customer behaviour and switching behaviour between technology products (e.g., Kamolsook et al., 2019). Leveraging the Diffusion of Innovations theory offered us a theoretical lens for exploring IoT technology in customer-facing environments. Yet, we integrated this with the Service-Dominant (SD) logic (Vargo & Lusch, 2004) in order to define and account for the service aspects. We consider this to be an important contribution. Our study offers evidence that combining the Diffusion of Innovations theory with an SD logic perspective can result in a more holistic understanding of the adoption and use of IoT by retailers, whereby both the technical and the service features of the solution are considered and examined. This is an important implication as there are numerous calls for research on the use of IoT within the retail sector and for the purpose of exploring smart technologies and their impacts on service and service innovations (Roy et al. 2017).

5.3 Implications for Practice

The present study offers important implications both to theory and practice by providing new knowledge on the concept of implementing IoT in a customer-facing environment adopting a pragmatic approach. To the best of our knowledge, this is one of the first studies to approach IoT security within the context of IoT implementation in a retail environment. Based on our findings, we have enhanced the existing IoT literature (Whitmore, Agarwal, and Da Xu, 2015; Li, Da Xu, and Zhao, 2015), offering a richer understanding of security in smart stores, informed by the Service-Dominant Logic, IoT network Security and the Diffusion of Innovations theory.

The study has further offered a comprehensive understanding of the practical considerations that companies need to take when implementing security for the IoT, such as the trade-off between security and costs. We offer a range of practical solutions and recommendations for the implementation of a customer-facing IoT system in-store. Among them, we consider the most critical that of the business case, which is often a factor for traditional IT projects (Kappelman et al., 2006). Companies should ensure that the reason for implementing the IoT is either for solving a business problem or for accessing a specific benefit, rather than simply because they 'want more technology'. This information should provide the basis for a business case that identifies the expectations of the project. While the usual InfoSec rules apply, for IoT in particular, companies should map out the data flows to identify the streams that require higher levels of protection and quantify them against a company-wide standardised scale.

With regards to data and devices, these should not be considered in isolation because the aggregate power of IoT data makes it as dangerous as it is useful. Equally, data collection for facilitating personalisation and analysis is very important for businesses. Indeed, the power of the IoT lies in its ability to contextualise the shop environment at an unprecedented level of granularity. Streamlining the collected data reduces the demand for storage and transmission, both of which are finite resources. In doing so, however, retailers will need to ensure that sensitive data is suitably encrypted when stored or transmitted. This poses a challenge as the demarcation of 'sensitive' and 'non-sensitive data gets blurred when data is collectively aggregated. This is of increased concern for businesses when considering IoT-enabled store environments, who will need to be confident and ensure that their security protocols and controls extend across their entire supply chain, including device suppliers and device manufacturers. Further, the retail sector is characterised by complex supply chains, whereby device suppliers and manufacturers often collaborate with hardware and software suppliers located in different countries where data protection regulations may differ considerably. Therefore, businesses will need to consider the potentially severe implications of non-compliance with local data protection regulations due to country-level inconsistencies.

5.4 Limitations and Future Research Direction

As with all empirical studies, the current study has its inherent limitations. Our study is an exploratory field study, and we collected our empirical material through semi-structured interviews. While our findings shed light on the implementation of IoT in the services industry, they cannot be generalised without caution. Primarily, we would propose their validation within a similar context and, from there, their extension to theory, as it is often the case with qualitative studies, which can, in turn, be validated and extended to different contexts (Davison and Martinsons, 2016, p. 247). In addition, we would welcome further research into the concept of and the effects of homogenising the device infrastructure both in terms of risk and quantifying benefits, which we think is essential, but outside the scope of this study. Although the concept of homogenising devices has been briefly examined here, it is essential to justify the validity of the concept through further research to assess the existence of any additional risks introduced by less variance in IoT devices. Furthermore, in the present study, security experts from different retail companies were interviewed regarding IoT implementation's drivers and security challenges in this specific industry. Future research should aim to capture the opinion and perspectives of marketing and customer insights professionals working in retail using IoT to understand customer security concerns better.

Another interesting avenue for further research would be to explore what makes a store environment synonymous with the concept of IoT, how IoT may be implemented together with other advanded technologies, such as the Blockchain, both for payments as well as for security purposes, and how would these influence customer and employee expectations in relation to security design and privacy expectations. In a world where businesses are expected to deploy ICTs ahead of their competition and be trendsetters, it would be interesting to see whether and to what extent an equal amount of care is expected or applied in making this offering secure by design. Previous studies have argued, for example, that in some cases Blockchain-powered systems can provide an additional layer of security (Zamani et al., 2020). Such a study could further focus on which types of IoT devices are most used in the retail sector, the particular security problems these devices imply and whether other compelementary technologies can address and improve perceived and real security issues. Finally, we note that in our study we explored the challenges and, more specifically, the security and privacy concerns of the implementing organization but also those of customers. As such, we did not examine aspects of performance; however, performance is highly linked with the identified challenges as any of these concerns can be directly affected. Future studies could explore this link through on the basis of a survey to identify, measure and explain the effect of security in IoT implementations and the direct/indirect links to performance.

6 Conclusion

This study aimed to explore the drivers and security challenges that organisations face when implementing an IoT in the store, focusing on the retail services industry sector. The retail industry is moving towards an experiential, personal provision for customers. In order to facilitate this, the IoT has been identified as a key technology that can sense and gather data from a store environment, streamline existing processes, and be used as a cost-effective and expedited way to effect the required change. At the same time, there are opportunities for a myriad of new services through the use of the IoT and market pressure and customers' expectations for many of these services. However, there are many challenges when it comes to the customer experience and the relevant security and privacy concerns but also for the organisations. As a future research agenda, these challenges need to be carefully considered before, during and after the implementation of the IoT system.

References

Accenture, 2017. Shaping the Future of Retail for Consumer Industries.

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

Aloysius, J.A., Hoehle, H., Goodarzi, S., Venkatesh, V., 2018. Big data initiatives in retail environments: Linking service process perceptions to shopping outcomes. Annals of Operations Research 270, 25–51. https://doi.org/10.1007/s10479-016-2276-3

Atzori, L., Iera, A., Morabito, G., 2010. The Internet of Things: A survey. Computer Networks 54, 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Balaji, M.S., Roy, S.K., 2017. Value co-creation with Internet of things technology in the retail industry. Journal of Marketing Management 33, 7–31. https://doi.org/10.1080/0267257X.2016.1217914

Ben-Asher, N., Meyer, J., Möller, S., Englert, R., 2009. An experimental system for studying the tradeoff between usability and security, in: Proceedings - International Conference on Availability, Reliability and Security, ARES 2009. pp. 882–887. https://doi.org/10.1109/ARES.2009.174

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K.N., Nadeau, E., O'Rourke, D.G., Piccarreta, B., Scarfone, K., 2019. Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks. Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.8228

Boyatzis, R.E., 1998. Transforming qualitative information: Thematic analysis and code development. Sage Publications, Inc., Thousand Oaks, CA, US.

Boyes, H., Hallaq, B., Cunningham, J., Watson, T., 2018. The industrial internet of things (IIoT): An analysis framework. Computers in Industry 101, 1–12. https://doi.org/10.1016/j.compind.2018.04.015

Bradlow, E.T., Gangwar, M., Kopalle, P., Voleti, S., 2017. The Role of Big Data and Predictive Analytics in Retailing. Journal of Retailing 93, 79–95. https://doi.org/10.1016/j.jretai.2016.12.004

Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qualitative Research in Psychology 3, 77–101.

Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. InternationalJournal of Information Management, 51, 101952. https://doi.org/10.1016/J.IJINFOMGT.2019.05.008

Bryman, Alan., Bell, E., 2011. Business Research Strategies, in: Business Research Methods. Oxford University Press, pp. 1–38.

D'Arcy, J., Herath, T., Shoss, M.K., 2014. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. Journal of Management Information Systems 31, 285–318. https://doi.org/10.2753/MIS0742-1222310210

Denyer, D., Tranfield, D., 2006. Using qualitative research synthesis to build an actionable knowledge base. Management Decision 44, 213–227. https://doi.org/10.1108/00251740610650201

Dijkman, R.M., Sprenkels, B., Peeters, T., Janssen, A., 2015. Business models for the Internet of Things. International Journal of Information Management 35, 672–678. https://doi.org/10.1016/j.ijinfomgt.2015.07.008

Edgar, T.W., Manz, D.O., 2017. Descriptive Study, in: Research Methods for Cyber Security. Elsevier, pp. 131–151. https://doi.org/10.1016/B978-0-12-805349-2.00005-4

ETSI, 2019. TS 103 645 - V1.1.1 - CYBER; Cyber Security for Consumer Internet of Things.

Fagan, M., Megas, K.N., Scarfone, K., Smith, M., 2019a. Core Cybersecurity Feature Baselinefor Securable IoT Devices: A Starting Point for IoT Device Manufacturers. Information Technology Laboratory. https://doi.org/10.6028/NIST.IR.8259

Fagan, M., Megas, K.N., Scarfone, K., Smith, M., 2019b. Core Cybersecurity Feature Baselinefor Securable IoT Devices: A Starting Point for IoT Device Manufacturers. Information Technology Laboratory. https://doi.org/10.6028/NIST.IR.8259

Giebelhausen, M., Robinson, S.G., Sirianni, N.J., Brady, M.K., 2014. Touch Versus Tech: When Technology Functions as a Barrier or a Benefit to Service Encounters. Journal of Marketing 78, 113–124. https://doi.org/10.1509/jm.12.0056

Gierej, S., 2017. The Framework of Business Model in the Context of Industrial Internet of Things, in: Procedia Engineering. Elsevier Ltd, pp. 206–212. https://doi.org/10.1016/j.proeng.2017.03.166

Goad, D., Collins, A.T., Gal, U., 2020. Privacy and the Internet of Things−An experiment in discrete choice. Information and Management. https://doi.org/10.1016/j.im.2020.103292

Gregory, J., 2014. The Internet of Things: Revolutionising the Retail Industry.

Greitzer, F.L., Kangas, L.J., Noonan, C.F., Dalton, A.C., Hohimer, R.E., 2012. Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats, in: 2012 45th Hawaii International Conference on System Sciences. IEEE, pp. 2392–2401. https://doi.org/10.1109/HICSS.2012.309

Grewal, D., Roggeveen, A.L., Nordfält, J., 2017. The Future of Retailing. Journal of Retailing 93, 1–6. https://doi.org/10.1016/j.jretai.2016.12.008

Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems 29, 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Hamilton, R., Ferraro, R., Haws, K. L., & Mukhopadhyay, A. (2021). Traveling with Companions: The Social Customer Journey. *Journal of Marketing*, *85*(1), 68–92. https://doi.org/10.1177/0022242920908227

Hennink, M.M., Kaiser, B.N., Marconi, V.C., 2017. Code Saturation Versus Meaning Saturation: How Many Interviews Are Enough? Qualitative Health Research. https://doi.org/10.1177/1049732316665344

Homburg, C., Jozić, D., Kuehnl, C., 2017. Customer experience management: toward implementing an evolving marketing concept. Journal of the Academy of Marketing Science 45. https://doi.org/10.1007/s11747-015-0460-7

Hoyer, W.D., Kroschke, M., Schmitt, B., Kraume, K., Shankar, V., 2020. Transforming the Customer Experience Through New Technologies. Journal of Interactive Marketing 51, 57–71. https://doi.org/10.1016/J.INTMAR.2020.04.001

Hu, S., Hu, B., & Cao, Y. (2018). The wider, the better? The interaction between the IoT diffusion and online retailers' decisions. Physica A: Statistical Mechanics and Its Applications, 509, 196–209. https://doi.org/10.1016/J.PHYSA.2018.06.008

Hui, S.K., Inman, J.J., Huang, Y., Suher, J., 2013. The Effect of In-Store Travel Distance on Unplanned Spending: Applications to Mobile Promotion Strategies. Journal of Marketing 77, 1–16. https://doi.org/10.1509/jm.11.0436

Hwang, Y. M., Kim, M. G., & Rho, J. J. (2015). Understanding Internet of Things (IoT) diffusion: Focusing on value configuration of RFID and sensors in business cases (2008–2012). Http://Dx.Doi.Org/10.1177/0266666915578201, 32(4), 969–985. https://doi.org/10.1177/0266666915578201

Inman, J.J., Nikolova, H., 2017. Shopper-Facing Retail Technology: A Retailer Adoption Decision Framework Incorporating Shopper Attitudes and Privacy Concerns. Journal of Retailing 93, 7–28. https://doi.org/10.1016/j.jretai.2016.12.006

Intel, 2017. The future of retail through the internet of things.

Jing, Q., Vasilakos, A. v., Wan, J., Lu, J., Qiu, D., 2014. Security of the Internet of Things: perspectives and challenges. Wireless Networks 20, 2481–2501. https://doi.org/10.1007/s11276-014-0761-7

Kamolsook, A., Badir, Y.F., Frank, B., 2019. Consumers' switching to disruptive technology products: The roles of comparative economic value and technology type. Technological Forecasting and Social Change 140. https://doi.org/10.1016/j.techfore.2018.12.023

Larivière, B., Bowen, D., Andreassen, T.W., Kunz, W., Sirianni, N.J., Voss, C., Wünderlich, N. V., De Keyser, A., 2017. "Service Encounter 2.0": An investigation into the roles of technology, employees and customers. Journal of Business Research 79, 238–246. https://doi.org/10.1016/j.jbusres.2017.03.008

Lazer, D., Kennedy, R., King, G., Vespignani, A., 2014. The Parable of Google Flu: Traps in Big Data Analysis. Science 343, 1203–1205. https://doi.org/10.1126/science.1248506

Lee, I., Lee, K., 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons 58, 431–440. https://doi.org/10.1016/j.bushor.2015.03.008

Lemon, K. N., & Verhoef, P. C. (2016). Understanding customer experience throughout the customer journey. Journal of Marketing, 80(6), 69–96. https://doi.org/10.1509/jm.15.0420

Lu, Y., Papagiannidis, S., & Alamanos, E. (2018). Internet of Things: A systematic review of the business literature from the user and organisational perspectives. Technological Forecasting and Social Change, 136, 285–297. https://doi.org/10.1016/J.TECHFORE.2018.01.022

Lusch, R.F., Nambisan, S., 2015. Service Innovation: A Service-Dominant Logic Perspective. MIS Quarterly 39, 155–175. https://doi.org/10.25300/MISQ/2015/39.1.07

Lusch, R.F., Vargo, S.L., 2006. Service-dominant logic: reactions, reflections and refinements. Marketing theory 6, 281–288.

Marikyan, D., Papagiannidis, S., Alamanos, E., 2020. Cognitive Dissonance in Technology Adoption: A Study of Smart Home Users. Information Systems Frontiers. https://doi.org/10.1007/s10796-020-10042-3

Marshall, M.N., 1996. Sampling for qualitative research, Family Practice © Oxford University Press.

Metallo, C., Agrifoglio, R., Schiavone, F., Mueller, J., 2018. Understanding business model in the Internet of Things industry. Technological Forecasting and Social Change 136, 298–306. https://doi.org/10.1016/j.techfore.2018.01.020

Ning, H., Liu, H., Yang, L.T., 2013. Cyberentity Security in the Internet of Things.

Ogunjimi, A., Rahman, M., Islam, N., Hasan, R., 2021. Smart mirror fashion technology for the retail chain transformation. Technological Forecasting and Social Change 173, 121118. https://doi.org/10.1016/J.TECHFORE.2021.121118

Palattella, M.R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T., Ladid, L., 2016. Internet of Things in the 5G Era: Enablers, Architecture, and Business Models. IEEE Journal on Selected Areas in Communications 34, 510–527. https://doi.org/10.1109/JSAC.2016.2525418

Pantano, E., Viassone, M., 2014. Demand pull and technology push perspective in technology-based innovations for the points of sale: The retailers evaluation. Journal of Retailing and Consumer Services 21. https://doi.org/10.1016/j.jretconser.2013.06.007

Patton, M.Quinn., 2002. Qualitative Interviewing, in: Qualitative Research and Evaluation Methods. Sage Publications, pp. 339–429.

Pauget, B., & Dammak, A. (2019). The implementation of the Internet of Things: What impact on organizations? Technological Forecasting and Social Change, 140, 140–146. https://doi.org/10.1016/J.TECHFORE.2018.03.012

Priporas, C.-V., Stylos, N., Fotiadis, A.K., 2017. Generation Z consumers' expectations of interactions in smart retailing: A future agenda. Computers in Human Behavior 77, 374–381. https://doi.org/10.1016/j.chb.2017.01.058

Ratna, V. V. (2020). Conceptualizing internet of things (IoT) model for improving customer experience in the retail industry. International Journal of Management, 11(5), 973–981. https://doi.org/10.34218/IJM.11.5.2020.089

Rogers, E.M., 2003. Diffusion of innovations. Free Press.

Roman, R., Najera, P., Lopez, J., 2011. Securing the Internet of Things. Computer 44, 51–58. https://doi.org/10.1109/MC.2011.291

Roy, S.K., Balaji, M.S., Sadeque, S., Nguyen, B., Melewar, T.C., 2017. Constituents and consequences of smart customer experience in retailing. Technological Forecasting and Social Change 124. https://doi.org/10.1016/j.techfore.2016.09.022

Shankar, S., Balasubramani, S., Basha, S., Ahamed, S., Reddy, N., 2021. Smart Trolley for Smart Shopping with an Advance Billing System using IoT, in: Proceedings of the Fifth International Conference on Computing Methodologies and Communication (ICCMC 2021).

Shankar, V., Kalyanam, K., Setia, P., Golmohammadi, A., Tirunillai, S., Douglass, T., Hennessey, J., Bull, J.S., Waddoups, R., 2021. How Technology is Changing Retail. Journal of Retailing 97, 13–27. https://doi.org/10.1016/j.jretai.2020.10.006

Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A., 2015. Security, privacy and trust in Internet of things: The road ahead. Computer Networks. https://doi.org/10.1016/j.comnet.2014.11.008

Sun, Y., Song, H., Jara, A.J., Bie, R., 2016. Internet of Things and Big Data Analytics for Smart and Connected Communities. IEEE Access 4, 766–773. https://doi.org/10.1109/ACCESS.2016.2529723

Suri, H., 2011. Purposeful sampling in qualitative research synthesis. Qualitative Research Journal 11, 63–75.

Tranfield, D., Denyer, D., Smart, P., 2003. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British Journal of Management 14, 207–222.

Vargo, S.L., Lusch, R.F., 2008. Service-dominant logic: continuing the evolution. Journal of the Academy of Marketing Science 36, 1–10. https://doi.org/10.1007/s11747-007-0069-6

Vargo, S.L., Lusch, R.F., 2004. Evolving to a new dominant logic for marketing. Journal of Marketing 68, 1–17.

von Briel, F., 2018. The future of omnichannel retail: A four-stage Delphi study. Technological Forecasting and Social Change 132, 217–229. https://doi.org/10.1016/j.techfore.2018.02.004

Walker, K.L., 2016. Surrendering Information through the Looking Glass: Transparency, Trust, and Protection. Journal of Public Policy & Marketing 35, 144–158. https://doi.org/10.1509/jppm.15.020

Wang, R.J.H., Malthouse, E.C., Krishnamurthi, L., 2015. On the Go: How Mobile Shopping Affects Customer Purchase Behavior. Journal of Retailing 91, 217–234. https://doi.org/10.1016/j.jretai.2015.01.002

Weber, R.H., 2010. Internet of Things - New security and privacy challenges. Computer Law and Security Review 26, 23–30. https://doi.org/10.1016/j.clsr.2009.11.008

Weber, R.H., Studer, E., 2016. Cybersecurity in the Internet of Things: Legal aspects. Computer Law and Security Review 32, 715–728. https://doi.org/10.1016/j.clsr.2016.07.002

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., Vasilakos, A. v, 2014. Security and privacy for storage and computation in cloud computing. Information Sciences 258, 371–386.

Whitmore, A., Agarwal, A., da Xu, L., 2015. The Internet of Things—A survey of topics and trends. Information Systems Frontiers. https://doi.org/10.1007/s10796-014-9489-2

Yee, K., 2004. Usability and Security. IEEE Security & Privacy 48–55.

Yun, H., Lee, G., Kim, D.J., 2019. A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. Information and Management. https://doi.org/10.1016/j.im.2018.10.001

Zamani, E., He, Y., & Phillips, M. (2020). On the security risks of the blockchain. Journal of Computer Information Systems, 60(6), 495-506.

Zamani, E.D., Pouloudi, N., Giaglis, G. *et al.* Accommodating Practices During Episodes of Disillusionment with Mobile IT. *Information Systems Frontiers* 23, 453–475 (2021). https://doi.org/10.1007/s10796-019-09972-4

Zhao, K., Ge, L., 2013. A survey on the internet of things security, in: Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013. pp. 663–667. https://doi.org/10.1109/CIS.2013.145