5-15-2019

TECHNOLOGICAL ENABLERS FOR PREVENTING SERVICE FAILURE WITH E-COMMERCE WEBSITES

Alireza Nili
Queensland University of Technology, a.nili@qut.edu.au

Alistair Barros
Queensland University of Technology, alistair.barros@qut.edu.au

David Johnstone
Victoria University of Wellington, David.johnstone@vuw.ac.nz

Mary Tate
Queensland University of Technology, mary.tate@qut.edu.au

TECHNOLOGICAL ENABLERS FOR PREVENTING SERVICE FAILURE WITH E-COMMERCE WEBSITES

Research paper

Nili, Alireza, Queensland University of Technology, Brisbane, Australia, a.nili@qut.edu.au

Barros, Alistair, Queensland University of Technology, Brisbane, Australia, alistair.barros@qut.edu.au

Johnstone, David, Victoria University of Wellington, Wellington, New Zealand, david.johnstone@vuw.ac.nz

Tate, Mary, Queensland University of Technology, Brisbane, Australia, mary.tate@qut.edu.au

Abstract

Problems with digital services still occur at times, even for the most reliable services. Considering the consequences of these failures and their effects on the customer's overall service quality perception and satisfaction, preventing these failures, and delivering reliable digital services, is a critical business competency. In addition, the fact that digital services are often co-produced by both service providers and their customers, shows the increasing role of both service providers and customers in preventing digital service failures (or service problems). In this study, we view the concept of digital service failure from the perspective of expectation-conformation theory, develop an Archimate architecture model and use it to design a typology of technological enablers (technologies and technological approaches) that can be used by businesses and their customers to prevent service failures at different stages of online purchase via e-commerce websites. The typology is relevant and useful for management information systems (MIS) academics and practitioners, particularly for information technology and digital service management researchers and the practitioner community.

Keywords: service failure, failure prevention, technological enabler, typology, ecommerce.

1 Introduction and Motivation

Digital service failures can and do occur, even for the most reliable services (Zhu et al., 2013; Dabholkar and Spaid, 2012). However, what constitutes "failure" may be different from an organizational and a customer perspective. In particular, not all instances where a service fails to meet customer expectations are recognized as a service failure. "Cart abandonment" while shopping online has been measured at an average of 75% of all transactions, and many of the reasons relate to failures to meet service expectations, for example, unexpected shipping costs (barilliance.com, 2018). Other examples of service failure from a user perspective include an e-commerce website with a long response time, confusing check-out, concerns about online payment transactions, and not receiving a purchased product or service properly or as the customer had expected. Preventing these failures, and delivering reliable digital services is a crucial business competency and helps to maintain a customer's overall satisfaction with these services. In this study, we focus on preventing failures with digital services that are offered via e-commerce websites, and develop a typology of technological enablers (technologies and technological approaches) that can prevent these failures. We answer the question "what are the technological enablers for preventing customer service failures with e-commerce websites?"

The concept of service failure is based on Expectation-Confirmation Theory (ECT: Oliver, 1980), and is defined as the gap between a customer's *perceived* quality of service delivery and his or her service expectations (Tan et al., 2016). ECT explains satisfaction with a service as a function of expectations,

perceived performance, and disconfirmation of beliefs. Expectations are the properties or characteristics of service performance the customer anticipates. Perceived performance is a person's perceptions of the actual performance of the service. There may be a difference – positive or negative – between what a person expects in a service, and their perceptions of what is delivered. The nature and direction of this gap influences their satisfaction (or dis-satisfaction) with the service (Oliver, 1980). However, studies of customer satisfaction with e-commerce websites (for example, Deveraj et al., 2002) frequently focus only on customer perceptions and "black box" the underlying technologies, that can contribute to – or prevent – service failure from a customer perspective. They are also frequently cross-sectional, and do not consider that customer expectations and perceptions of service may be different as they move through the value-chain of seeking, selecting, purchasing, and so on. These are the gaps we address.

We note that in this study, by e-commerce websites, we mean online shopping websites. A contemporary categorisation of service failures that is highly relevant to e-commerce websites is provided by Tan et al. (2016), who categorise these failures into: information, functional, and system failures. Information failures happen when the information that is available or is generated by the website is incapable of guiding customers to use website functionalities and accomplish transactions (for example, when information is inconsistent, not accurate or incomplete). Functional failures happen when the functionalities provided on the website (e.g. payment options or features enabling customers to customise an item) are unable or insufficient to support customers in the purchase of an item. Finally, system failures are the situations where the functionalities provided on the website are not delivered properly (e.g. the system is inordinately slow in access or is temporarily unavailable, due to problems in the network security or processing of an order).

Overall, many digital service failures happen due to technical errors, such as network or security errors. Recalling the concept of perceived service failure based on ECT, a fast and automatic recovery of these errors, *before* they affect the service delivery process, can prevent them from becoming a service failure in the minds of customers. This is the reason why we consider some technologies that include fast and automatic error recovery (particularly for recovering errors in network) among the technologies for service failure prevention. Some service failures cannot be prevented at the time, but some analytical technologies can help businesses prevent similar failures occurring in the future. Finally, a service failure could also occur from the customer perspective without a real technical problem, for example due to inaccurate or out-dated information about website functionalities. Some technologies (e.g. various forms of social media and conversational interfaces) can help customers and businesses to interact in a way that can prevent this group of service failures, or minimise the probability of them occurring.

Considering the negative effects of a service failure on customers' perceived quality of service, satisfaction, consequent word-of-mouth communication and potential reputational damage (Dabholkar and Spaid, 2012; Tan et al., 2016), preventing service failure and delivering reliable digital services is important for online businesses. Enterprise architectural views of service failure prevention and risk management studies and technology governance frameworks such as COBIT, usually have an organizational, rather than a customer experience focus. To our knowledge, this is the first study to link customer perceptions of service with underlying technologies.

In the rest of the paper we explain why and how we designed our Archimate architecture for e-commerce website use as a process in three layers, where the first layer (business layer) is the basis for designing the second layer (application layer), and the second layer becomes the basis for designing the third layer (technology layer). We explain how we identified four categories of technologies in the technology layer, which were then considered as the criteria for organising 'prevention' technological enablers within the typology. Next, we explain how we conducted an extensive literature review to identify the technological enablers, and how our typology was formed by organising these enablers based on the four categories of technologies in the technology layer of the Archimate diagram. Then, we explain how we validated the typology. Because digital services are often co-produced by both service providers and their customers, and because both providers and customers are increasingly expected to prevent digital service failures, in our typology we identify which technological enablers can be used by businesses and which ones can be provided by businesses to be used by their customers. The typology also shows which of the enablers can be used to prevent which of the three types of service failure. We present the typology

diagrammatically, and then supplement this with more detailed information in a series of tables. We believe that the typology is particularly useful for information technology and digital service management researchers, as well as the practitioner community.

2 Method

In this section, we explain how and why we designed our Archimate architecture for e-commerce websites, how we conducted a literature review to identify the technological enablers and how our typology was formed by organising these enablers based on the technology layer of the Archimate architecture. We then explain how we validated the typology by seeking feedback from practitioner experts in the field.

2.1 Designing the typology

2.1.1 Designing a criteria for the typology

In typology design, researchers design 'a' typology, not 'the' typology, since each researcher can use a range of different and unique properties for categorisation purposes (Marradi, 1990). In order to design our typology, we needed to develop a suitable criteria to organise the prevention technological enablers. In this paper, we focus on our previous work (Nili et al., 2014) and Aulkemeier et al.'s (2016) work on e-commerce reference architecture to develop a value-chain (rather than cross-sectional) view of the customer experience of e-commerce services that can then be linked to underlying architectures.

Aulkemeier et al.'s (2016) service-oriented e-commerce architecture was designed to be a comprehensive Archimate architecture for e-commerce research and practice. An Archimate architecture is a modelling language that supports the analysis of an enterprise architecture (business activities and the related back-end applications and technologies). Aulkemeier et al.'s (2016) architecture, however, mostly focuses on the e-commerce back-end infrastructure. On the other hand, in our prior work (Nili et al., 2014), we developed a 'service value chain' framework for e-commerce websites explicitly from both the customer and business perspectives, and showed how the back-ends of e-commerce applications and technologies can be designed based on the inter-section of these two perspectives. In order to design the 'service value chain' framework, we drew from Ives and Learmonth's (1984) and Ives and Mason's (1990) original customer service lifecycle framework, Burt and Sparks (2003) and Elliott et al.'s (2010) process frameworks, and Alter's (2008, 2010) service value chain framework, and used it to inform our criteria for organising prevention technologies in the typology. A digital service value chain represents the sequential steps required to produce a final outcome in a digital service setting. In the e-commerce context, more specifically in the online shopping context, the online purchase of an item is often the outcome. Figure 1 presents the service value chain framework that we developed in our prior work, including the use of a website for online purchases, starting from need/want recognition and ending with post-purchase evaluation by customers.

Because of the focus of this study and the concept of service failure (based on ECT), we adapted the service value chain (Figure 1) for this study by slightly revising its steps into: (1) information search (such as brands, prices, features, etc about one or more type of product or service on the website); (2) evaluation of options (considering their brands, quality, features, etc.); (3) completion of customer information (e.g. customer's name, identifying information and postal address if needed); (4) online payment; (5) purchase receipt (e.g. via email or a message on the screen); (6) delivery of the service or product (e.g. download of a digital product or postal delivery); and (7) post-purchase evaluation (e.g. evaluation of quality of service delivery via a customer feedback form available on the website). This seven-step process became the basis for our design of an Archimate architecture for online purchase via e-commerce websites. The Archimate architecture was then used as our criteria for organising the technological enablers in the typology.

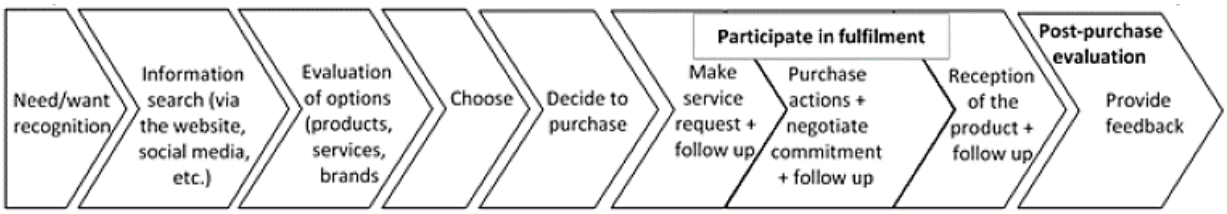

Figure 1. Digital service value chain for e-commerce websites from the customer's perspective [adapted from Nili et al. (2014)]

There are several languages and modelling tools such as Orbus, Sparx, ARIS, ERwin, Dragon and Archimate, some of which are mostly useful for enterprise architects or for system architects, some have been designed for software developers and some straddle these groups. We chose using Archimate, as it suits the purpose of this study. A complete Archimate diagram includes three layers: (1) a 'business' layer, which presents the process of producing products and services for external customers. It could be realised as a business process performed by business actors in an organisation to produce a service, or it could be realised as the process of using a self-service technology (e.g. e-commerce websites) by customers themselves; (2) an 'application' layer, which includes software and application services that support the process in the business layer in an automated way; and (3) a 'technology' layer, which includes communication and system software that offer infrastructure services such as the data storage and processing required to run applications in the application layer. The seven-step process of online purchase (adapted from Figure 1) constitutes the business layer of our Archimate architecture for e-commerce websites.

We conducted a two and half hour workshop-style brainstorming session with seven experts in developing Archimate architecture for e-commerce websites. Each expert has at least five years of industry experience and has taught enterprise architecture in academia for at least four years. In the brainstorming session, using a top-down approach, we first presented the business layer (the seven-step online purchase process) to the experts. Once all experts fully agreed with the components and their sequence in the business layer, we used the layer as the basis for designing the application layer in the architecture. To do this, we asked the experts to identify and organise software and application services that are required for supporting the steps in the business layer based on their knowledge, experience and a comparison with Aulkemeier et al.'s (2016) model. Using the same approach, the technology layer was then designed by including the communication and system software that are required to run and support the software and application services in the application layer. Having designed the technology layer, we found that the technologies in this layer can be organised into four main categories including: technologies related to 'application services', 'business process services', 'data storage and access services' and 'security management services'. *These four categories in the technology layer were used as the criteria for designing our typology.* Finally, as we explain below, we conducted an extensive literature review to identify and locate prevention technological enablers based on their usefulness and relevancy to each of the four categories in the technology layer.

2.1.2 Literature review to identify and include technological enablers in the typology

We reviewed information systems, computer science, electronic commerce and service management literature to identify any technology or technological approach that can, or has a clear potential to, prevent website service failures. To do this, we used Templier and Paré's (2015) framework, which provides a systematic and transparent approach to guide the literature review. The steps of the framework include: (1) Specifying the purpose of literature review (the aim was to identify specific technologies and technological approaches that can prevent service failures with e-commerce websites or the technologies that clearly have the potential to do so); (2) Searching the literature through a clear search procedure (see below); (3) Screening for inclusion (we selected or excluded the identified papers based on their relevance to our research question, i.e. based on whether they provide information on technological enablers); (4) Assessing the quality of studies (we considered all journal and conference papers, as the six databases provide high quality papers); (5) Extracting relevant information from the

selected papers (we extracted technological enablers and their definitions from the selected papers); and (6) Synthesising the findings (we organised the enablers based on their usefulness and relevancy to the four categories in the technology layer).

We searched for relevant material in journals, conferences and books within the ACM Digital Library, the AIS Electronic Library, ProQuest Computing, SpringerLink, Web of Science and ScienceDirect databases, employing the following search terms: service failure; service problem; service recovery; service failure prevention, service problem prevention, e-commerce service failure, and e-commerce service problem. Journal and conference papers were considered regardless of their rank. This resulted in a large number of search hits (447 studies), which were refined by checking the title and abstract of each paper. After three rounds of paper selection, 37 papers were found to be relevant. Next, we did forward and backward citation checking of the selected papers and identified 3 new relevant papers. After reviewing all selected papers, we identified 43 technological enablers. These were organised according to their usefulness and relevancy to the four categories of technology services in the technology layer, forming the final draft of the typology. Finally, by reviewing the text of these papers, we identified and reported which of the three types of service failures each of these technological enablers can prevent. References to the source papers are also provided (in Tables 1 to 4) for readers to access more in-depth technical descriptions of the technological enablers. In our literature review, we also realised that enterprise architectural views of service failure prevention usually have a technical, or organizational, rather than a customer experience focus. For example, Liu et al. (2010) focus on issues of scalability, reliability and reusability, without linking them to customer satisfaction. Other, more comprehensive risk management and technology governance frameworks, such as COBIT-5, focus on enterprise risk in a very broad sense, not specifically on the risk of failing to meet customer expectations. Our review of literature and design of the typology fills this gap by linking customer perceptions of service with underlying technologies for customer service failure prevention.

2.2 Validating the typology

We then validated our typology by seeking individual feedback from eight different experts in the field. Each expert has at least five years of practitioner experience in the field of computer information systems and e-commerce (in the area of service design for online shopping). We sent our architecture and the typology to the experts via email or visited them in person and asked them to revise the steps in the online purchase process in the business layer, the elements in the application and technology layers, and the relationships between the layers in the architecture (Figure 2). We then asked them to add, remove or revise the enablers in the typology (Figure 3 and Tables 1 to 4) based on the suitability of the enablers for preventing service failures that had previously occurred for online shopping via their websites. Overall, the only changes were a slight clarification in the wording of a process step in the business layer by one participant in the IS discipline and a slight clarification in the wording of a prevention technology by another participant in the same field. These two minor changes were confirmed by the other participants.

Note that, if required, an additional and more detailed layer could be designed for each of the four categories in the technology layer of the Archimate diagram. For example, a recent study by Pursky and Mazoha (2018) provides a detailed view of the business process management component. We stopped going into further level of details, as we had reached a point that is sufficient for using the architecture as our criteria for designing the typology. This was also confirmed by all experts. Also, while a separate set of technologies could be identified to prevent the failure of prevention technological enablers in the typology, all experts commented that the typology covers all enablers that are directly relevant to the four categories in the technology layer and are the ones that are required for effective customer service failure prevention.

3 Results

Figure 2 presents the three layers, including the business layer, application layer and technology layer of our Archimate architecture for online shopping via e-commerce websites. As mentioned, the four

categories of technology services in the third layer were used as the criteria to organise prevention technological enablers in the typology. These four categories are shown in a red and dashed rectangular in the figure.

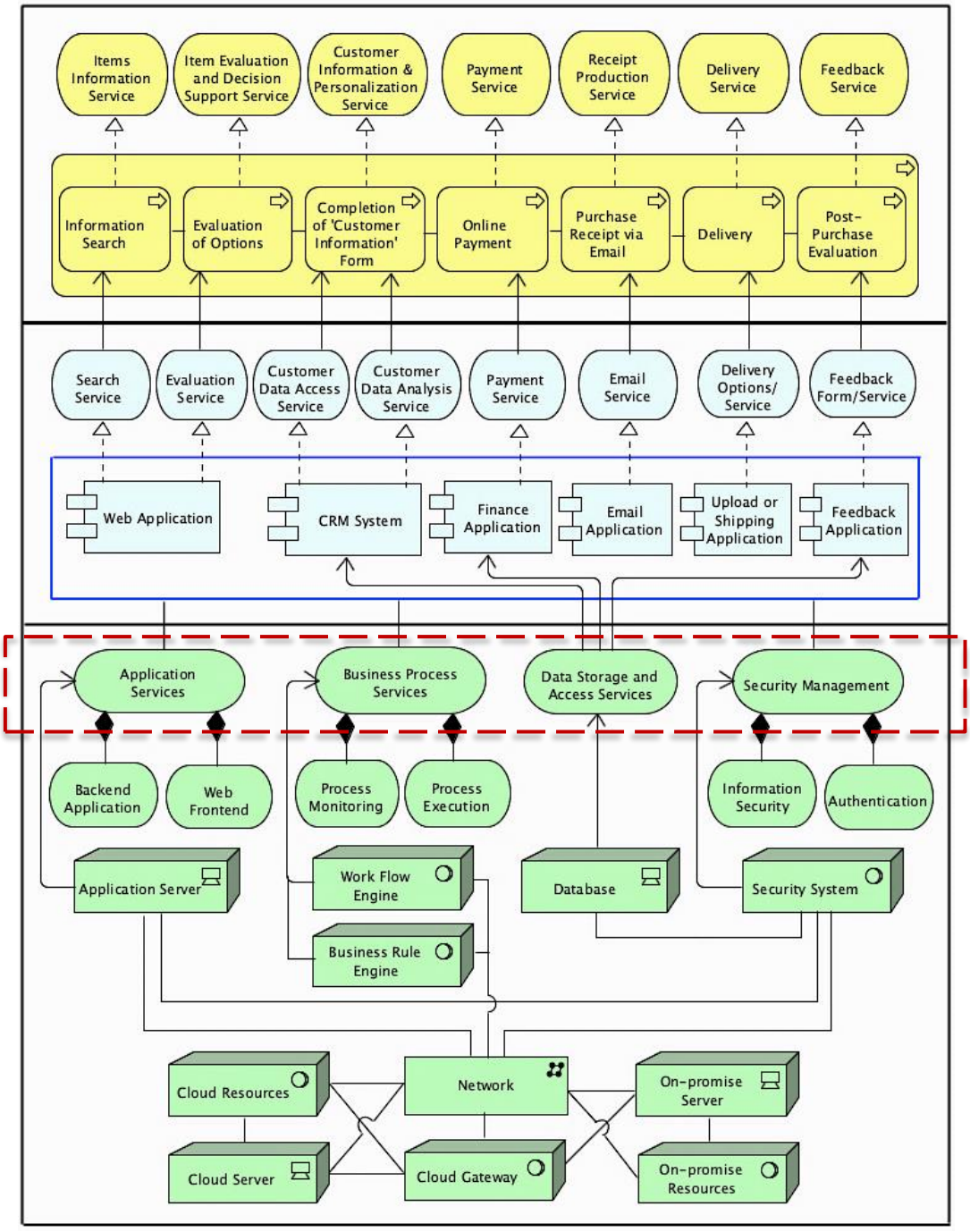

Figure 2. An Archimate architecture for online purchase via e-commerce websites.

We remind readers that the ultimate purpose of presenting the technologies in the technology layer is to present a technology infrastructure that supports running the applications in the application layer. Presenting information about what specific technologies are used in the layer, such as specific technologies of data storage and access services (e.g. types of databases, Data SET/Data Reader, ADO.NET and Language Integrated Query: LINQ) is out of the scope and aim of Archimate architecture and this paper.

Figure 3 presents our typology, in which the prevention technological enablers we identified from literature are organised according to their usefulness and relevancy to the four categories of technology services in the technology layer. We note that the typology does not present the technical components that form a technological enabler. For example, it does not aim to present technical details such as natural language processing, machine learning and conversation management that form an AI-based chatbot.

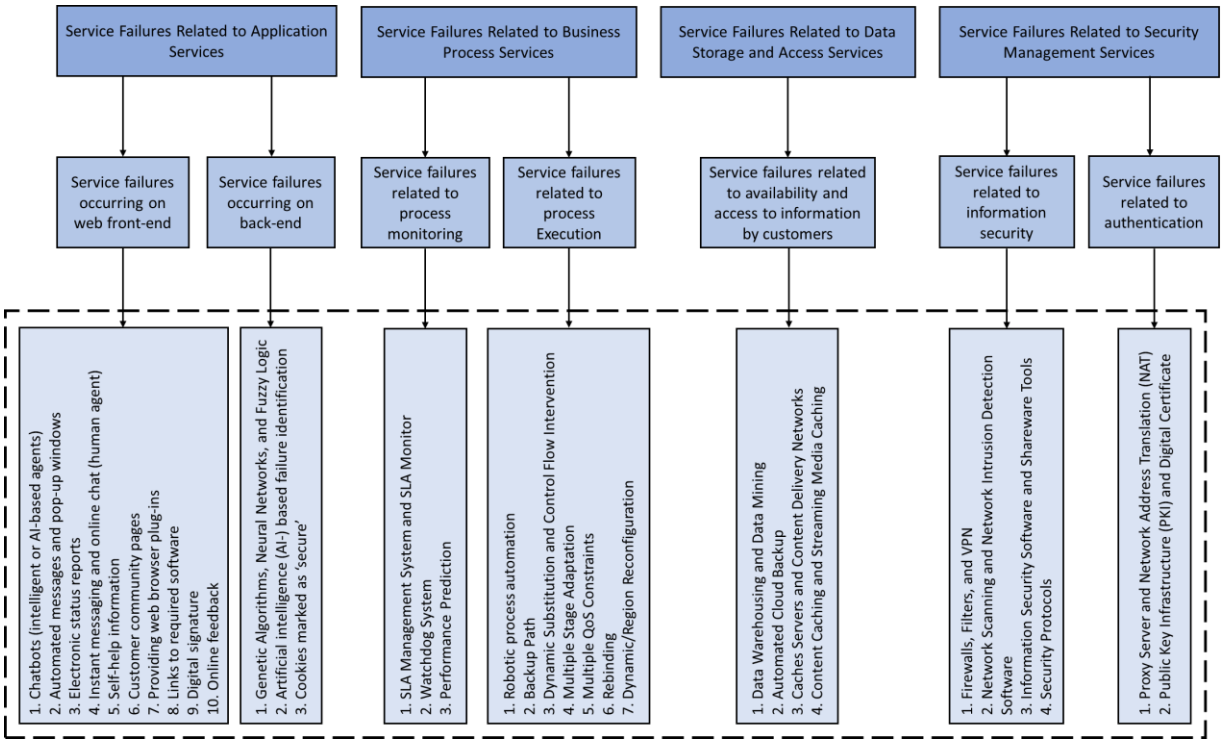

Figure 3. A typology of technological enablers for service failure prevention with e-commerce websites

Tables 1 - 4 present a brief description of the technological enablers (technologies and technological approaches) that businesses or their customers need to use to prevent service failures with e-commerce websites, what type or types of service failures each of them can prevent, and the corresponding source references to provide more detailed technical descriptions.

As shown in Figure 2 and Figure 3, technological enablers that can support prevention of service failures that are related to application services are categorised into two groups, including: technological enablers to support prevention of failures on the web front end and technological enablers to support prevention of failures on back end. Table 1 presents the description and related references for these enablers, both on the web front end (these enablers can be provided by the business for their customers) and on the back end (these enablers can be used by the business).

Prevention Enablers Related to Application Services			
Prevention enablers related to web front-end [to be provided for customers]			
Prevention Enabler	**Description**	**Type of failure to be prevented**	**Source**
Chatbots (intelligent or AI-based agents)	Intelligent (AI-based) agents that work via natural language processing and machine learning can offer 24/7 service support questions in a natural and conversational language	Information failure	Davenport, and Ronanki (2018); Nili et al. (2019)
Automated messages	To provide guidance and directions on the current and the next steps of the purchase process	Information failure	Kasabov and Warlow (2009); Shaw and Craighead (2003); Kimes and Collier (2015)
Electronic status reports	Automated emails or messages on a screen about the current or next steps of a service process	Information failure	
Instant messaging and online chat capabilities with human agents	Instant messaging and online chat capabilities sessions with service support staff for customer enquiries and questions	Information failure	
Self-help information	Including online instructions, Frequently Asked Questions (FAQs) and video tutorials	Information failure	
Customer community pages	A part of the website dedicated for provide and receive support from other users	Information failure	
Providing web browser plug-ins	To give a web browser a required functionality, such as displaying some types of content the browser was not originally designed to display.	Information and functional failures	Kasabov and Warlow (2009); Shaw and Craighead (2003); Yu et al. (2008)
Links to required software	Including links to downloading a compatible web browser, a required software or their latest version.	Information and functional failures	
Digital signature	Assists in verifying the contents of purchase documents and the sender's identity.	Information failure	
Online feedback	An online feedback form, customers' community pages on the website, and links to service provider's social media for customer feedback on service delivery	Information and functional failures	Kasabov and Warlow (2009); Challagalla et al. (2009)
Prevention enablers related to web backend [to be used by business]			
Prevention Enabler	**Description**	**Type of failure to be prevented**	**Source**
Genetic Algorithms, Neural Networks, and Fuzzy Logic	To help with classifying and route the causes of service failures (root cause analysis) for design improvement and to prevent their repeated occurrence in the future.	Functional and system failures	Shaw and Craighead (2003); Borrajo et al. (2011); Davenport, and Ronanki (2018)
Artificial intelligence (AI-) based failure identification	AIs can help earmark and analyse data related to failures to prevent them in future. AI can also help businesses to identify potential occurrence of fraud (fake identities or fraudulent payments/transactions)	Functional and system failures	
Cookies 'marked as secure'	Using the cookies that store encrypted user data and passing them through the Secure Socket Layer (SSL) security protocol to store authentication and user information and preferences	Information and functional failures	Niranjanamurthy and Chahar (2013)

Table 1. Prevention technological enablers for application services

Table 2 presents the description and related references for prevention technological enablers related to business process services, including enablers related to process execution and enablers related to process

monitoring. Both types of technological enablers can be used by the business, due to their implementation at the back end of the overall system.

Prevention Enablers Related to Business Process Services [to be used by business]			
Prevention enablers related to process execution			
Prevention Enabler	**Description**	**Type of failure to be prevented**	**Source**
Robotic process automation	The approach uses 'robots' for inputting and integrating service transaction and customer interaction data from multiple channels, such as website and mobile app into systems of record.	Functional and system failures	Davenport, and Ronanki (2018)
Backup Path	If the optimal path of service delivery fails to accomplish the purpose, the current and future executions can continue through a second path.	Functional and system failures	Yu and Lin (2005); Feng et al. (2007)
Dynamic Substitution and Control Flow Intervention	An automatic service substitution at runtime in a service composition that dynamically replaces faulty services by semantically equivalent ones	Functional and system failures	Moller and Schuldt (2010)
Multiple Stage Adaptation	Helps the system react effectively to the changes in network configurations and quality of service (QoS) offerings by employing a different type of service for a fast compensation of a failed service.	Functional and system failures	Chafle et al. (2006)
Multiple QoS Constraints	Web services are usually a composition of multiple technical services from multiple providers with different QoS and Service Level Agreements (SLAs). The approach dynamically finds a new path that starts from the preceding service by maximising or minimising some QoS values.	Functional and system failures	Feng et al. (2007); Laleh et al. (2018)
Rebinding	In case a service is unavailable, the approach helps early run-time re-binding for functionally equivalent services in a service composition.	Functional and system failures	Canfora et al. (2008)
Dynamic/Region Reconfiguration	Using an iterative algorithm, the approach dynamically replaces a faulty service by some of its neighbouring services in the region of that QoS.	Functional and system failures	Lin et al. (2010)
Prevention enablers related to process monitoring			
Prevention Enabler	**Description**	**Type of failure to be prevented**	**Source**
SLA Management System and SLA Monitor	SLA monitor ensure that the service fulfils the QoS requirements of SLA by observing the runtime performance. SLA management system processes and uses this data for SLA reporting metrics.	Functional and system failures	Mosallanejad et al. (2014)
Watchdog System	Dynamically and periodically checks the signals sent through software or hardware components, monitors the attempts to access website and informs service providers of website access failures.	Functional and system failures	Ibrohimovna and Groot (2010)
Performance Prediction	A fast self-healing that finds a backup during the execution in the changing Web environment (e.g. data transmission speed that can affect QoS).	Functional and system failures	Dai, Yang and Zhang (2009)

Table 2. Prevention technological enablers for business process services

Next, Table 3 presents the description and related references for prevention technological enablers related to data storage and access services. Similar to the previous table, these enablers can be used by the businesses only.

Prevention Enablers Related to Data Storage and Access Services [to be used by business]			
Prevention Enabler	**Description**	**Type of failure to be prevented**	**Source**
Data Warehousing and Data Mining	Separate databases can be used for maintaining 'value failure data' and to help analysis of service failures to prevent their repeated occurrence in future.	Information, functional, and system failures	Demirkan and Delen (2013)
Automated Cloud Backup	Reduces the threat of hardware failures, outages and natural disasters that lead to data loss and severe service failures. Also, Hybrid Cloud, a relatively new solution for small businesses, can replicate snapshots of servers and workstations to the Cloud.	Information, functional, and system failures	Chang et al. (2016)
Caches Servers and Content Delivery Networks	By placing cached servers between the origin servers and customers in content delivery network, e-businesses can move and store frequently requested contents closer to their customers. This reduces the traffic to the origin server and makes handling the purchase process with less waiting time and delay.	Information, functional, and system failures	Lamberti and Sanna (2007); Napier et al. (2003)
Content Caching and Streaming Media Caching	Storing and moving frequently requested content closer to users to reduce traffic to the original server and handling of the requests more quickly (content caching). A similar approach for downloading video and audio content is called Streaming Media Caching.	Information, functional, and system failures	Lamberti and Sanna (2007); Napier et al. (2003)

Table 3. Prevention technological enablers for data storage and access services [to be used by business]

Finally, Table 4 presents the description and related references of technological enablers which can support preventing failures that are related to security management. Similar to the two previous tables, these enablers can be used by the businesses only.

Prevention Enablers Related to Security Management [to be used by business]			
Prevention Enabler	**Description**	**Type of failure to be prevented**	**Source**
Firewalls, Filters, and VPN	Firewalls (can be categorised as packet-filtering, circuit-level, and application-level firewalls), filters (block the spurious traffic in a distributed denial of service attack), and VPN (a combination of firewalls, digital certificates, and public and private key encryption) can assist with preventing security related failures.	Functional failure and system failure	Chang et al. (2016); Gehling and Stankard (2005); Kizza (2013); Moradian and Håkansson (2006); Niranjanamurthy and Chahar (2013); Rane et al. (2012); Shah (2002)
Proxy Server and Network Address Translation (NAT)	Proxy Servers and NAT can be separately used to protect user's IP address in the event of a security issue with the network.	Functional failure and system failure	Kizza (2013); Gehling and Stankard (2005); Niranjanamurthy and Chahar (2013); Shah (2002)
Network Scanning and Network Intrusion Detection Software	Assist with vulnerability monitoring by a continuous scanning and finding potential risks that match the characteristics of the known threats in a 'threat database', analysing patterns of suspicious behavior and/or developing Threat Models to help preventing exploits in future.	Functional failure and system failure	Napier et al. (2003); Tyagi and Srinivasan (2011); Marchany and Tront (2002); Yasin et al. (2012); Niranjanamurthy and Chahar (2013); Kizza (2013); Chomsiri (2007)
Information Security Software and Shareware Tools	Assist with website traffic analysis, proxy server reporting, monitoring and recovery for limited or unlimited number of connected devices to a network, quality control, and securing payment systems.	Functional failure and system failure	Tyagi and Srinivasan (2011); Marchany and Tront (2002); Yasin et al. (2012)
Security Protocols	Protocols such as Secure Socket Layer (SSL) and Transport Layer Security (TLS) for securing communication channels, and the protocols such as Secure Payment Application (SPA), Secure Electronic Transactions (SET), 3D Secure and e-Cash for securing online payments	Functional failure and system failure	Niranjanamurthy and Chahar (2013); Yasin et al. (2012); Kizza (2013); Manakshe et al. (2014)
Public Key Infrastructure (PKI) and Digital Certificate	PKI creates digital certificates, securely stores them in a public repository, allows businesses (who use a digital certificate) to check the public keys of other businesses in the network, and disproves a certificate if it is not valid anymore.	Functional failure and system failure	Napier et al. (2003); Tyagi and Srinivasan (2011); Kizza (2013)

Table 4. Prevention technological enablers for security management

4 Discussion and Conclusion

We developed an Archimate architecture model and used it as a set of criteria to design a typology of technological enablers that can be used to prevent service failures at different stages of online purchase via e-commerce websites. Because digital services (in this paper – online shopping via e-commerce websites) are often co-produced by both service providers and their customers, both service providers

and customers are increasingly expected to prevent digital service failures. Therefore, in our typology we identified which technological enablers can be used by businesses and which ones can be provided by businesses to be used by their customers. The typology also shows which of the enablers can be used to prevent which type of service failure (information failure, functional failure and/or system failure). Our contribution is to provide a theoretically grounded linkage between customer perceptions (satisfaction and dis-satisfaction) with e-commerce services, including a "life-cycle" view of service value, with the underlying technologies that can prevent negative experiences of expectation disconfirmation at various stages. While our Archimate diagram is a contribution to the IS field by itself, our typology of technological enablers (which is also a result of an extensive review of literature) is the main contribution of this paper. Our paper contributes to effective management of digital services by bridging technical and managerial (customer service) perspectives on preventing digital service failures.

The main limitation of this study is that we only focused on preventing digital service failures, which are offered via e-commerce websites. Considering the increasing number of studies on multi-channel services and omni-channel service interactions (seamless and integrated experience of using multiple channels of service delivery), we suggest future research to study digital service failure prevention in these service environments. Of course, designing a typology like the one we have designed may be more challenging for such service environments, where multiple channels are used for one service. However, such research can consider various related issues, such as preventing digital service failures with a focus on adaptability of channels (the channel tunes itself) and consistency of information (e.g. access to personalised information) when a user aims to use a service through different channels via different devices (e.g. smartphones and laptops) and networks.

Implementation of the prevention technological enablers is a must-do activity and not just a nice-to-do, as it certainly can support service failure prevention and reduce the probability of customer dissatisfaction and reputational risks for the business. Businesses can also choose to defray the risk by building and increasing redundancy into the infrastructure or by paying and pushing the provision of failure prevention (or the infrastructure supporting these services) to a managed services provider and let them absorb the risk.

In this study we viewed the concept of digital service failure from the perspective of Expectation-Confirmation Theory and considered a service failure as any 'perceived service failure' from the customer perspective. Such a perspective, led us to consider some technologies and technological approaches that include fast and automatic error recovery (particularly, for detecting and recovering errors in network before they become a service failure in the customer's mind) among the technological enablers for service failure prevention. Therefore, using a different theory or model in the digital service management area may result in designing a different typology with a different level of complexity and content. In addition, the tables in our typology show that the majority of enablers that prevent information and system failures can prevent functional failures, as well. Therefore, future research can study root causes of functional failures in detail, and could also argue that an information failure or a system failure could be a cause of a functional failure. We also encourage researchers to investigate the managerial (in additional to the technological) enablers for preventing digital service failures.

References

Alter, S. (2010). "Viewing systems as services: a fresh approach in the IS field." *Communications of the Association for Information Systems* 26 (11), 194-224.

Alter, S. (2014). "Work system perspective on service, service systems, it services, and service science." *Business Analytics and Information Systems.* Paper 45.

Aulkemeier, F., Schramm, M., Iacob, M. E. and Van Hillegersberg, J. (2016)."A service-oriented e-commerce reference architecture." *Journal of Theoretical and Applied Electronic Commerce Research 11*(1), 26-45.

Barilliance.com (2018). Complete List of Cart Abandonment Statistics: 2006-2018. URL: https://www.barilliance.com/cart-abandonment-rate-statistics/ (visited on 03/28/2019).

Borrajo, M. L., Baruque, B., Corchado, E., Bajo, J. and Corchado, J. M. 2011. "Hybrid neural intelligent system to predict business failure in small-to-medium-size enterprises." *International Journal of Neural Systems* 2 (4), 277-296.

Burt, S. and Sparks, L. (2003). "E-commerce and the retail process: A review." *Journal of Retailing and Consumer Services* 10 (5), 275-286.

Canfora, G., Di Penta, M., Esposito, R. and Villani, M. L. (2008). "A framework for qos-aware binding and re-binding of composite web services." *Journal of Systems and Software* 81 (10), 1754-1769.

Chafle, G., Dasgupta, K., Kumar, A., Mittal, S. and Srivastava, B. (2006). "Adaptation in web service composition and execution." *IEEE International Conference on Web Services*, 549-557.

Challagalla, G., Venkatesh, R. and Kohli, A. K. (2009). "Proactive postsales service: When and why does it pay off?" *Journal of Marketing* 73 (2), 70-87.

Chang, V., Kuo, Y. H. and Ramachandran, M. (2016). "Cloud computing adoption framework: A security framework for business clouds." *Future Generation Computer Systems* 57, 24-41.

Chomsiri, T. (2007). "Https hacking protection." *Advanced Information Networking and Applications Workshops, IEEE*, 590-594.

Dabholkar, P. A. and Spaid, B. I. (2012). "Service failure and recovery in using technology-based self-service: Effects on user attributions and satisfaction." *The Service Industries Journal* 32 (9), 1415-1432.

Dai, Y., Yang, L. and Zhang, B. (2009). "Qos-driven self-healing web service composition based on performance prediction." *Journal of Computer Science and Technology* 24 (2), 250-261.

Davenport, T. H. and Ronanki, R. (2018). "Artificial intelligence for the real world." *Harvard Business Review*, 96 (1), 108-116.

Demirkan, H. and Delen, D. (2013). "Leveraging the capabilities of service-oriented decision support systems: Putting analytics and big data in cloud." *Decision Support Systems* 55 (1), 412-421.

Deveraj, S., Fan, M. and Kohli, R. (2002). "Antecedents of B2C channel satisfaction and preference: Validating e-commerce metrics. *Information Systems Research*, 13 (3), 316-333

Feng, X., Ren, Y., Hu, J., Wu, Q. and Jia, Y. (2007a). "A model for service composition with multiple Qos constraints." *International Conference on Computing: Theory and Applications*, IEEE, 208-213.

Feng, X., Wang, H., Wu, Q. and Zhou, B. (2007b). "An adaptive algorithm for failure recovery during dynamic service composition." *International Conference on Pattern Recognition and Machine Intelligence*. Springer Berlin Heidelberg, 41-48.

Gehling, B. and Stankard, D. (2005). "Ecommerce security." *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development*, 32-37.

Ibrohimovna, M. and de Groot, S. H. (2010). "Reputation-based systems within computer networks." *International Conference on Internet and Web Applications and Services*, 96-101.

Ives, B. and Learmonth, G. P. (1984). "The information system as a competitive weapon." *Communications of the ACM* 27 (12), 1193-1201.

Ives, B. and Mason, R. O. (1990). "Can information technology revitalize your customer service?" *Academy of Management Perspectives* 4 (4), 52-69.

Kasabov, E. and Warlow, A. J. (2009). "Automated marketing and the growth of 'customer compliance' businesses." *Journal of Direct, Data and Digital Marketing Practice* 11 (1), 30-35.

Kimes, S. E. and Collier, J. E. (2015). "How customers view self-service technologies." *MIT Sloan Management Review* 57 (1), 25-26.

Kizza, J. M. (2013). *Guide to Computer Network Security*. 2nd Editio. Springer-Verlag London.

Laleh, T., Paquet, J., Mokhov, S. and Yan, Y. (2018). "Constraint verification failure recovery in web service composition." *Future Generation Computer Systems*, 89, 387-401.

Lamberti, F. and Sanna, A. (2007). "A streaming-based solution for remote visualization of 3d graphics on mobile devices." *IEEE Transactions on Visualization and Computer Graphics* 13 (2), 247-260.

Lin, K. J., Zhang, J., Zhai, Y. and Xu, B. (2010). "The design and implementation of service process reconfiguration with end-to-end Qos constraints in Soa." *Service Oriented Computing and Applications* 4 (3), 157-168.

Liu, D., Deters, R. and Zhang, W. J. (2010). "Architectural design for resilience." *Enterprise Information Systems* 4 (2), 137-152.

Manakshe, A. R., Jirkar, S., Wakhare, P. and Buram, V. (2014). "Analysis of secure electronic transmission (Set) system for electronic transactions." *International Journal of Research in Advent Technology* 2 (3), 12-15.

Marchany, R. C. and Tront, J. G. (2002). "E-commerce security issues." *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, 2500-2508.

Marradi, A. (1990). "Classification, typology, taxonomy." *Quality and Quantity* 24 (2), 129-157.

Moller, T. and Schuldt, H. (2010). "Osiris next: Flexible semantic failure handling for composite web service execution." *International Conference on Semantic Computing*, 212-217.

Moradian, E. and Håkansson, A. (2006). "Possible attacks on Xml web services." *International Journal of Computer Science and Network Security*, 154-170.

Mosallanejad, A., Atan, R., Murad, M. A. and Abdullah, R. (2014). "A hierarchical self-healing SLA for cloud computing." *International Journal of Digital Information and Wireless Communications* 4 (1), 43-52.

Napier, H. A., Judd, P., Rivers, O. and Adams, A. (2003). *E-Business Technologies*. Boston, MA: Thomas Course Technology.

Nili, A., Barros, A. and Tate, M. (2019). "The public sector can teach us a lot about digitizing customer service." *MIT Sloan Management Review*, 60 (2), 84-87.

Nili, A., Tate, M. and Gable, G. (2014). "A typology of technological enablers of website service failure prevention." *Pacific Asia Conference on Information Systems*, Chengdu, China.

Niranjanamurthy, M. and Chahar, D. D. (2013). "The study of e-commerce security issues and solutions." *International Journal of Advanced Research in Computer and Communication Engineering* 2 (7), 2885-2895.

Oliver, R. L. (1980). "A cognitive model for the antecedents and consequences of satisfaction." *Journal of Marketing Research* 17 (4), 460-469.

Pursky, O. and Mazoha, D. (2018). "Architecture model of integrated web-based e-trading business process management system." *International Journal of Information Engineering and Electronic Business*, 10 (2), 1-8.

Rane, P. B., Kulkarni, P., Patil, S. and Meshram, B. B. (2012). "Authentication and authorization: Tool for ecommerce security." *Engineering Science and Technology: An International Journal* (2:1), 150-157.

Shah, S. (2002). Top Ten Web Hacks. *Black Hat Asia. Singapore*. URL: *https://www.blackhat.com/presentations/bh-asia-02/bh-asia-02-shah.pdf* (visited on 15/01/2017).

Shaw, N. G. and Craighead, C. W. (2003). "Technology enablers to recover from failures in e-services." *Communications of the ACM* 46 (6), 56-57.

Tan, C. W., Benbasat, I. and Cenfetelli, R. T. (2016). "An exploratory study of the formation and impact of electronic service failures." *MIS Quarterly* 40 (1), 1-29.

Templier, M. and Paré, G. (2015). "A Framework for guiding and evaluating literature reviews." *Communications of the Association for Information Systems*, 34, Article 6.

Tyagi, N. K. and Srinivasan, S. (2011). "Ten-stage security management strategy model for the impacts of security threats on e-business." *International Journal of Computer Applications* 21 (5), 1-4.

Yasin, S., Haseeb, K. and Qureshi, R. J. (2012). "Cryptography based e-commerce security: A review." *International Journal of Computer Science Issues* 9 (2), 132-137.

Yu, Q., Liu, X., Bouguettaya, A. and Medjahed, B. (2008). "Deploying and managing web services: Issues, solutions, and directions." *The VLDB Journal—The International Journal on Very Large Data Bases* 17 (3), 537-572.

Yu, T. and Lin, K. J. (2005). "Adaptive algorithms for finding replacement services in autonomic distributed business processes." Autonomous Decentralized Systems, Isads 2005. Proceedings. IEEE, 427-434.

Zhu, Z., Nakata, C., Sivakumar, K. and Grewal, D. (2013). "Fix it or leave it? Customer recovery from self-service technology failures." *Journal of Retailing* 89 (1), 15-29.