# Development and Deployment of a Simple Ecommerce Website

Kevin Zoltán Barta

# Contents

# 1 Introduction

## 1.1 Short Description of the Task

The goal is to produce a simple yet robust and extendable ecommerce website which includes a frontend/backend part and a database. The website should have the core functionalities of an ecommerce website, such as creating an account, logging in and placing orders. Additional functionalities may be added; however, the focus is on the core functionalities and their stability.

## 1.2 Definition of Ecommerce

Ecommerce stands for electronic commerce. Commerce refers to the trade of goods and the activities associated with this. [1] Although ecommerce has several definitions [2], in this paper we accept the simplified definition of trading goods through electronic communication and activities related to that. [3] Ecommerce may be business-to-business (B2B), business-to-consumer (B2C) and even consumer-to-consumer (C2C). [1, 3] In our case, we will be focusing on the business-to-consumer model, since this website intends to sell goods to the broad public. As opposed to brick-and-mortar stores, ecommerce sites typically do not have physical premises.

## 1.3 History of Ecommerce

### 1.3.1 Early Attempts

A core concept to cover in the advent of ecommerce is the Electronic Data Interchange (EDI), which allows the automated exchange of documents between businesses. This technology appeared in the middle of the 1970s. Even though the functionalities EDI offered, it did not spread rapidly, more than 20 years past its appearance, by the late 1990s, less than 1% of the companies in Europe and the United States had adopted this technology, due to its costliness and complexity. [3]

Not long after the beginning of EDI, in the late 1970s, EFT (Electronics Funds Transfer) appeared, which enabled electronic transfers. In case of the United States, these transfers happen under the Automated Clearing House (ACH) system. According to data from 2019, the ACH system handles 24 billion transactions every year. [4] In 1979, Michael Aldrich invented teleshopping, which can be considered as a predecessor of today's ecommerce. [4, 5]

One of the first attempt of ecommerce as we know today was in 1984, when CompuServe, at that time the main provider of bulletin boards, introduced the Electronic Mall, which offered the goods of more than 100 stores. The service did not become popular. [6]

### 1.3.2 New Generation of Ecommerce

In the early 1990s, with the appearance of the graphical user interface, the Internet started to gain traction with the general public. This process led the Internet, once a tool for researchers and engineers, to start growing into a business-oriented technology. A good illustration of this is the fact that in 1997 the commercial (.com) domain took over the educational (.edu) domain in terms of popularity, as the most widely used top-level domain. From an ecommerce perspective, the 1991 lifting of commercial restrictions imposed on the network by NSFNET marked an undoubtably important event, allowing the establishment of non-governmental ISPs. [2]

Once ecommerce began its spread, the next obstacle for further growth was limited Internet access and security concerns. With the help of new legislation and agreements, the security concerns were (at least partly) addressed. [3] In 1993, the Secure Socket Layer (SSL) protocol was created, which laid the foundation of secure data transfer online. Not long thereafter appeared the first third-party credit card processing companies, which marked a significant event in the development of ecommerce. [6]

In 1995 Amazon appeared in the ecommerce scene as a bookstore, followed by eBay, a hybrid consumer-to-consumer and business-to-consumer trading platform, two months later. The rapid growth of ecommerce can be illustrated by the fact that the market in the United States more than doubled in its value between 1997 and 1998, growing from $2.6 billion revenue to $5.8 billion. An even more startling example is Amazon's growth in sales from just $16 million in 1996 to $1.6 billion in 1999. Even during the dot-com crash, ecommerce sales still increased. [3]

In the 2010s, ecommerce experienced rapid growth. In 2013, China exceeded the United States in online sales, making it the world's largest ecommerce market. China experienced a 33.3% growth of expenditure in online sales in 2015, the same year, the United States experienced a 14.6% growth. [5] The role of social media also became more prominent for businesses. Companies started to develop more direct connections with their consumers, to give a personal touch to their products, in an attempt to gain and retain more customers. [4]

## 2  Literature Review

### 2.1  UI Best Practices

To learn about the best practices in UI, I am drawing inspiration from two of the most famous UI-related books: Steve Krug's *Don't Make Me Think, Revisited* and Adam Wathan & Steve Schoger's *Refactoring UI*.

#### 2.1.1  Takeaways from "Don't Make Me Think"

In case of Steve Krug's Don't Make Me Think, Revisited, the author focuses on usability and emphasizes that the principles he lays down may already be known by the reader, however they may not be actively applied during their workflow.

It is crucial to keep the design intuitive, so that the user can recognize what action they need to take without having to actively think about it. Using this approach can save the user both time and effort. We should aim to make the website self-evident and where that is not possible, we should aim to make it at least self-explanatory. [7] An example I could think of where self-evident approach may not work in case of an ecommerce site, is when we need to integrate a third party service, such as payment or package tracking. In this case, we are dependent on a service that is not managed by us; thus, we may have to explain its usage in advance if it happens to have bad design or if possible, write some form of a wrapper around it, keeping the original business logic, with our custom UI (this however could be challenging due to legal reasons).

Users try to avoid reading and just skim through the websites as fast as possible with a goal in their mind. [7] For this reason, we should not turn our website into a reading assignment. This is often due to the consideration that clicking the wrong button has lower opportunity cost (potentially a few more clicks) than reading the website carefully (inherently time-consuming activity). The most important takeaway is to avoid ambiguity as users tend to click on the first button that appears to be matching their target. A classic source of ambiguity in case of ecommerce sites is between signing up and logging in. Our goal with a website is typically not to teach the user how to use it, since that is not what they come for, instead we must focus on keeping it obvious so that the user does not have to read a novel in order to find their target.

An important principle of design is that there is no need to reinvent the wheel, it is better to follow conventions where it makes sense. In some specific situations it can be beneficial to break conventions but in the vast majority the cases, it is better to stick to them. Creating visual hierarchy is a great way to group elements and draw attention to the most important parts of the site (e.g., by using a larger font or a color that stands out). This technique existed even before the Internet, for example in newspapers. Segmentation of the text is also

important; people prefer reading the same text broken down to paragraphs instead of all at once. [7] This not only groups related thoughts together but also allows the reader to take a break, if necessary, between two paragraphs.

Krug calls against being verbose on the Internet. Needless words must be eliminated, since people typically hurry on websites, minimizing their time to read. Navigation on the Internet compared to the physical world can be more challenging, due to the lack of scale, sense of location and direction. This can be tackled to some degree by establishing site hierarchy. Some parts are displayed on every page of the website, typically those located in the header and the footer, e.g., the site ID (name and logo of the website), navigation section and utilities (such as the search bar, the login button or the about page). The page must indicate clearly where we currently are on the site. Sub-levels can add complexity to the site and designers of the website often fall into the pitfall of not giving enough significance to the lowest level, albeit the users spending an equal amount of time on the lowest pages as the home page. Displaying the current page is also really important to provide the user a good sense of location on the site and the possibility to easily return next time. [7]

The homepage has to establish the identity of the site. Relevant content is also important, since outdated content indicates that the site has been abandoned. Juggling between the balance of what the user needs and what we want to showcase may prove tricky, but it is essential to maintain usability while also encouraging the user to discover more. Once visiting the home page, the user needs to quickly understand what the page is about. For this purpose, Krug suggests using a tagline, which is a short description that describes what the site is about, typically next to the site ID. [7]

Throughout the book Krug emphasizes the importance of usability. Usability tests provide incredibly valuable insights from the users, that the designers and developers might miss throughout the development process. This process consists of a user trying the website and the development and design team (or a usability engineer) taking notes of user's remarks and what they are doing on the website. It is recommended to conduct these tests periodically throughout the development cycle, to notice and fix design mistakes as soon as possible. The goal of this qualitative test is typically not finding all the flaws of the website but the most prominent ones. [7]

Krug starts off talking about UI design for mobiles by stating that the same basic principles apply here too. Development for mobile devices (responsive design) can be challenging, due to the space constraints. The most important features must be the most easily accessible ones. It is important to note that certain actions, such as hover, are not available on mobile devices. Due to these limitations, the user interface may not be as intuitive as on the desktop version,

the goal is to make it easy to learn and memorable, so that the user does not feel discouraged opening the website on their phone. [7]

Unfortunately, it is common to forget about accessibility, but on a larger website, it is inevitable to include in the design. Krug mentions that the most common reasons why accessibility gets overlooked is: not being affected by a disability, not being in a social circle where people are affected by any disability, due to the extra work and compromises in the design. While it is true that adding accessibility features can be complex, it is not always the case. Simply adding alt texts for images, which indicate what can be seen on the image for blind users (and also serve as the text in the tooltip of the image), using the label element in case of forms to associate an input field with the appropriate text label and adding a high contrast theme are relatively simple steps that can be taken towards a more accessible website. [7]

## 2.2 Cloud Deployment and Security

### 2.2.1 Security Concerns
Common security concern customers have with ecommerce is about the confidentiality of their transactions, unauthorized use of their credit cards, fraud, misuse of their data and many others. There are four main requirements for data safety: [8]

- Privacy – only authorized parties should have access to the information.
- Integrity – the message cannot be altered.
- Authentication – the sender and the recipients must identify themselves.
- Non-repudiation – proof that the target received the message.

Kalamkar mentions two more important aspects: [9]

- Confidentiality – prevention of unauthorized access.
- Availability – the user should be able to access the resources they are authorized to.

Hussain also mentions access control in this list, stating that only authorized persons should have access to the resources, [10] which coincides with the definition used by Padmannavar for privacy. [8] Sun et al. also mention these principles in their own words. [11] Yang et al. also mention most of these principles while adding a few others, such as fine-grained access control, secure data sharing in a dynamic group, leakage-resistance and complete data deletion. [12]

It is important to comply with these principles throughout the data life cycle, which Chen and Zhao describe as follows: [13]

Generation → Transfer → Use → Share → Storage → Archival → Destruction

Chen and Zhao mention valuable considerations regarding cloud security, namely that the multi-tenant nature of the cloud makes it difficult to determine what resources have been compromised in case of a security risk. In case an organization uses multiple providers for provisioning different resources, it is difficult to unify security measures. The multi-tenant nature of the cloud poses a threat of unauthorized users accessing the data of other tenants. They also emphasize that cloud security measures must meet the needs of massive information processing. [13]

### 2.2.2 Common Security Threats

Hussain outlines seven main threats for ecommerce security: [10]

- Authentication Attacks – when an unauthorized user alters the system. This may happen through shared passwords or unattended open sessions. Brute-forcing the passwords on resources could be another way of getting access.
- Integrity Attacks – when the data is tampered with during transition. An example when this can be exploited is if a program does not check the buffer limit, allowing the attacker to add arbitrary data after the limit. This allows the attacker to slow down or completely shut down system by flooding it with data.
- Confidentiality Attacks – an example would be getting access to data using a packet sniffer program.
- Virus - malicious computer programs that are designed to replicate themselves and spread to other computers when triggered by a certain event. A network can get infected by a virus from an outside source. Once a computer is infected within the network, the other computers are also at a high risk of being affected.
- Trojan Horse – these malicious pieces of code are disguised as useful programs and require the user to download them. Once installed, the system of the user is compromised.
- Worms – malicious programs that spread through computer networks. They are designed to replicate themselves, e.g., by sending copies of themselves in an email attachment. They can create security risks by opening TCP ports, or flood the network, initiating a Denial-of-Service attack.
- Database Threats - some database systems store the username/password pair in a non-secure way, if an attacker gets access to these credentials, they gain access to private information in the database.

Al Ladan breaks down the security threats of ecommerce platforms to three different levels: [14]

- Client level

- Frontend server and application level
- Network and backend server level

One of the vulnerabilities on the client level is devices connected to wireless networks. Password-protecting the network can help mitigate the risks, however wired networks are still considered more secure. Possible attacks on wireless networks include: [14]

- Replay attack – the attacker can capture and retransmit a message, even to a different destination.
- Eavesdropping – the attacker can capture and read sensitive data if it is not encrypted.
- Pull attack (on cellphones) – the attacker has full control over the mobile device.
- Push attack (on cellphones) – the attacker plants malicious code on the mobile device which spreads that to other devices in the network.
- Lost device – although not an attack, it is still an important aspect to consider, that in case a device gets lost, malicious actors should not be able to access sensitive data.

Server exploits are the most dangerous threats on the frontend server/application level, wherein attackers can gain administrator access. Attacks the hackers can launch on this level include: [14]

- Buffer overflow – when the allocation of storage is not handled properly by a program, the attacker can make use of this vulnerability tricking the server into executing some malicious code.
- Software bugs – a common reason behind security holes is unskilled or careless developers, who leave mistakes in their code, creating a new vulnerability. Solving this problem is not trivial, since ecommerce platforms should be interoperable with external systems, adding more complexity. Following standards could provide a solution, although it is worth noting that even the standards and protocols can keep changing rapidly, which makes staying up-to-date a difficult task.
- Viruses and malicious software – viruses and malicious software can infect ecommerce platforms various ways, causing significant losses, steal sensitive data or make the platform, or a part of it, inaccessible.

Networks are dependent entities; they depend both on the private network, which is often owned and managed by others (e.g., in a cloud environment), and the public network, where control over security is lacking. These factors contribute to security issues, where the most common issues are: [14]

- Session interception – the session can be obtained by an attacker, e.g., in case of a man in the middle attack, where the attacker places a malicious host between the client and the server.
- Cross-site scripting (XSS) – attackers can place malicious code inside the content served on a website. Because the browser detects the ecommerce site as a trusted source, the inserted code operates with the same permissions, which the attackers can exploit.
- Firewall loophole – firewalls separate the backend servers from the corporate network. Since they are typically implemented at a network level, they do not protect against attacks on a higher level (e.g., HTTP which is in the application layer). This means that, for example, a buffer overflow attack could be carried out in this layer.

### 2.2.3 Mitigation of The Security Risks

With the help of encryption, it is possible to address privacy concerns. [8, 13] One method for this is using PKI (public key infrastructure), which consists of a public/private key-pair, where the public key encrypts the message and the private key decrypts it. The public key, as the name implies, is publicly distributed, while the private key is kept hidden by the recipient. This technology forms the bases of the RSA cryptosystem and the PGP encryption. PKI is not fit for encrypting large amounts of data, for this reason it is typically only used for agreeing upon a key, thereupon using symmetric encryption. [8] Symmetric encryption can be really fast and have a low complexity [10, 13], allowing easy implementation, however it requires a shared secret that the parties agreed on previously. [10] Unfortunately, encrypting stored data is not always a viable option. In case of static data, it can lead to problems with indexing and querying. [13]

Although credit card details can be transferred through SSL safely, the server storing credit card details poses a security risk. MasterCard and Visa developed a protocol, SET (Secure Electronic Transaction) [8, 14], which authenticates the three parties involved in the transaction, namely the bank, the merchant and the customer. This protocol prevents the merchant from storing any sensitive information on their server. There are three transactions happening during a credit card payment: [8]

- Credit card details transferred to the merchant or payment gateway
- Credit card details forwarded to the bank from the merchant
- Order and customer details provided to the merchant from the payment gateway/credit card company

Digital signatures serve as a way to verify the origin of online transactions. It is best compared to a physical signature. Besides providing proof of the origin, the digital signature also assures the recipient that the data has not been altered. [10]

Digital certificates allow parties to prove their identity. They use an electronic key to encrypt and sign digital information. These certificates are issued by a Certificate Authority and signed by the authority's private key. [10]

Smart cards are plastic cards with similar dimensions to traditional debit and credit cards. There are two main categories of these, microprocessor cards and memory cards. The purpose of these cards is helping with authentication. They are called smart, due to their capability of data processing and the algorithms stored on them. [10]

Electronic money is payment on the Internet resulting in money transferred from one account to another. The transaction contains data, encrypted by the merchant's private key, about the amount spent, a serial number, the identity of the buyer and expiry. The transaction is recorded to ensure that the same money is not spent twice. Once the issuer verifies the serial number, to ensure that the money is not double-spent, they add the amount on the merchant's bank account. [10]

### 2.2.4 Cloud Storage

Cloud computing is the on-demand offer of applications and resources as services over the Internet. The National Institute of Standards and Technology (NIST) defines cloud computing as "*cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*". [11]

NIST differentiates three service models (also called the SPI model):

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Based on access scope we differentiate three cloud categories: [11]

- Public – property of a service provider, it may be accessed by everyone.
- Private – property of a company, only accessible by authorized parties.
- Hybrid – a mix between public and private.

NIST differentiates an additional deployment model, called community cloud. [13]

Cloud storage allows the storage and sharing of data in the cloud. It has the advantage of unlimited space, convenience, safety, possibility of backups and low cost. Cloud platforms typically offer three types of storage: [12]

- Block storage – data broken down to fixed blocks and only reassembled once the user retrieves them. It is the default storage method on hard drives and can be used on Storage Area Networks (SANs). Block storage is not capable of storing metadata, making it unfit for unstructured data. It is also a popular choice for deploying virtual machine file system (VMFS). [15]
- File storage – data saved in files, e.g., network-attached storage (NAS) and even an ordinary hard drive uses file storage. It uses a hierarchical structure of folders. [15]
- Object storage – large volumes of unstructured data, all the objects are at the same level. It can also store metadata associated with the object. Each object can be accessed using a unique number. The files can only be managed via an API. [15]

Cloud storage consists of four layers: [12]

- Storage layer
- Primary management layer
- Application interface layer
- Access layer

### 2.2.5 Data Security in the Cloud

Data security has been a major concern in the IT field. Data security in the cloud is more complicated than in a traditional environment since the data is scattered over different machines and storage devices. Protecting the data of the users is crucial to gain their trust. [11, 14] While cloud computing can save time and money for a company, they must trust the service that they are using, since the most important asset of a company is the data that they manage. [11] Surveys from the early days of cloud support this: in a 2009 survey conducted by IDCI 74% IT managers and CIOs stated that the primary challenge for the adaptation of cloud computing was security issues. Another survey from 2009, by Gartner, further proves this, where more than 70% CTOs mentioned privacy and security concerns as the main preventive factor of cloud adaption. [13]

Sun et al. focus on four different data security aspects: integrity, confidentiality, availability and privacy. [11]

Data integrity refers to the protection of the data from unauthorized altering, fabrication or removal. In case of a standalone system, this is not a complex task and can be achieved simply using database constraints and transactions. Most importantly these transactions must have ACID (atomicity, consistency, isolation, and durability) properties. In a cloud context the key component of data integrity is properly managed authorization. To verify the integrity of the data, Proofs of Retrievability can be adopted, which uses a combination of error correction code and spot-checking. The HAIL (high-availability and integrity layer)

12

builds on top of Proofs of Retrievability, which provides a way to check data in different clouds, ensuring availability and integrity. [11] Another technique is provable data integrity (PDI, developed by NEC Labs) [13], where the client fingerprints the data and uploads the fingerprint along with the data to the cloud platform, then whenever the client wants to check the integrity of the data, it sends a "challenge" to the server and compares the received data with the expected output. [16]

Data confidentiality is pivotal for users to store private and confidential data in the cloud. Sun et al. call against storing sensitive data in the cloud, even if encryption is in place, due to the possibility of human errors, such as improper key management, while also criticizing the lack of fine-grained authorization. [11] Chen and Zhao also emphasize the importance of key-management, while bringing up the issue that users lack expertise, which makes them rely on the key-management of the cloud provider, that in turn makes the cloud provider's responsibility more complex due to the increasingly large volume of keys they need to manage. Access control is also crucial, the mobility of the employees is relatively high, meaning that systems should be able to quickly provision and deprovision accounts, to avoid unauthorized access by employees who left the organization. [13]

Homomorphic encryption ensures that the algebraic operations on the clear text remain the same even after encryption, which means that the text does not have to be decrypted first. [11, 13] This technique can help preserve the confidentiality of the data while undergoing data operations in the cloud. Fully homomorphic encryption allows any operation on the data without having to decrypt, however the computational complexity and the amount of storage it requires still makes it impractical as of 2014. [11]

Due to the inefficiency of full homomorphic encryption, researchers started focusing on limited homomorphic encryption, where only the most common operations, such as the search operation, are possible without decryption. In-memory database encryption utilizes a synchronizer which provides the key to the client, to decrypt the data it wants to access. The drawback of this approach is the delay that the synchronizer adds however this issue can be addressed by minimizing the communication between the nodes and the synchronizer. [11]

Distributive storage can help with ensuring the integrity of the data while also providing data privacy. One such technique is breaking the data into chunks, encrypting these parts and uploading them to different databases. With the help of tailored measurements, it is possible to adjust the provisioned resources according to the user's need based on the outgoing and incoming traffic. [11]

A hybrid technique can be applied to achieve both data confidentiality and data integrity. It utilizes both key sharing and authentication techniques. RSA can be used for the key

exchange between the user and the cloud provider. A three-layer model may be followed, in which the first layer handles authentication, the second layer is responsible for encryption of the data and the third layer is used for data recovery. [11]

Data concealment is a technique to achieve data confidentiality, by mixing real data with fake data, which only the authorized users can differentiate. This increases the overall volume; however, it enhances security. Watermarking can be used to differentiate real data. [11]

Deletion confirmation means that once the user confirms that they want the data to be deleted, it is actually deleted and not recoverable. This means all the copies of the data have to be deleted at the same time, in a way that it is not possible to recover the deletion. Encryption also helps here, e.g., using the FADE (file assured deletion) system, data is encrypted before it is uploaded to the cloud and it assures that the file is unrecoverable after deletion. [11]

Data availability refers to the availability and recoverability of data in case of accidents (e.g., natural disasters or hardware issues) or network failure. Cloud computing adds a level of complexity to data storage, since cloud clients have to comply with local laws in the country where the servers are based. [11]

### 2.2.6   Data Privacy in the Cloud

The Canadian Institute of Chartered Accountants (CICA) defines privacy in the Generally Accepted Privacy Principles (GAPP) as *"The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information."* [13]

Privacy is the idea of control over one's private information and the ability to reveal information selectively. Sun et al. outline four main categories of privacy issues: [11]

- Enabling users to have control over their data and preventing data theft, selling and misuse.
- Avoiding data loss and keeping consistency during data replication.
- Clarifying the responsible party for the legal requirements.
- Finding the extent cloud providers are involved in processing the data.

Service abuse is an important issue in the world of cloud computing. A good example of this is deduplication, when the same data is shared by different users, and the cloud provider stores only one copy of it, to save on storage. Another form of service abuse is when the attacker tries to deplete the resources of the cloud provider, by overloading the resources, incurring extra costs for the client or the cloud provider. [11]

### 2.3   Analyzing Existing Ecommerce Platforms

This section focuses on three main ecommerce platforms: Alibaba, Amazon and eBay. The choice is not arbitrary, the intention was to showcase the differences between B2B (Alibaba), B2C (Amazon) and C2C (eBay) ecommerce sites. For the sake of completeness, a self-hosted platform (WooCommerce) will also be included. It is worth noting that while Amazon and Alibaba have many other services, the focus will be on their core websites: A mazon.com and Alibaba.com.

### 2.3.1 Alibaba

Alibaba was founded by Jack Ma in 1999 who served as the chairman and chief executive officer of the company until 2013. The company's growth coincides with the spread of internet in China. [17]

The Alibaba Group has many subsidiaries, including Chinese retail markets such as Taobao, Tmall, Juhuasuan, a Chinese wholesale market called 1688.com, the global version of the site called Alibaba and the retail version of Alibaba, AliExpress. [17]

Besides ecommerce sites, the Alibaba Group also has payment services (Alipay), a logistics information system (China Smart Logistics), online marketing services (Alimama) and even a cloud computing provider (Alibaba Cloud Computing). [17]

Alibaba assists small exporters, primarily based in China, in finding businesses who can source their products. While Alibaba does not have commission fees, they do make a profit by membership fees (membership determines the number of products sellers can showcase [highlight] and the number of RFQ responses [request for quotation] per month). A custom pricing model is used to determine the membership fees. [17, 18] Most of the company's revenue comes from advertising. According to data from 2014, Alibaba reported a gross merchandise volume of $296 billion, exceeding eBay and Amazon combined. [19]

A typical deal is made with the following workflow from the buyer's perspective:

Sign up → Set up business details → Find the needed products → Request a quote from the sellers/ask for clarification (e.g., about shipment) → Evaluate quotes and select the best one → (Optionally) Create a trade assurance contract if possible (if the seller is a Trade Assurance supplier, for handling disputes) → Pay for the product/deposit (in case the product is not readily available, the rest will be paid later). This process can be done through online banks, credit card, telegraphic transfer or Payment Terms (offered by Alibaba in the United States) with different transaction fees. → Shipping → Inspect the received products (optionally conduct pre-shipment product inspection) [20]

Shipping is handled by a freight service. Alibaba offers the following shipping methods: [20]

- Ocean Freight – buyers can choose from two container options, FCL (full container load) or LCL (less than container load), the former fit for high volume orders, where an entire container can be filled with the order, and the latter for low volume orders, so that the buyers can save money.
- Air Express & Air Parcel – a cost effective airborne shipping method that is available for products of suppliers based in China.
- Air Freight – also known as air cargo, it is designed for orders between 150 and 500 kg. It is a time-sensitive and more expensive shipping option. The shipping rate is calculated from the cargo's actual weight and dimensional weight, where the larger one becomes the chargeable weight.

Dimensional weight is calculated using the following formula: $(length \times width \times height) \div (dimensional\ weight\ factor)$, where the dim factor (dimensional weight factor) is the volume of package allowed per unit of weight. For example, if the minimum weight allowance per m$^3$ is 50 kg, then the dim factor can be calculated dividing the volume by the weight: $\frac{1\ m^3}{50\ kg} = 0.02\ m^3/kg$. If the order in question has a weight of 20 kg with the following dimensions (in meter): $0.5 \times 0.5 \times 2$ then the volume is 0.5 m$^3$. In this case, even though the actual weight is only 20 kg, the dimensional weight is $(0.5 \times 0.5 \times 2) \div 0.02 = 25\ kg$, meaning that rate will be calculated based on the dimensional weight.

### 2.3.2 Amazon

Amazon was founded in 1994 by Jeff Bezos. In the early days, the company was focused entirely on the sale of books, which is why it was headquartered in Seattle, due to the proximity of the Oregon book distribution center. Soon, Amazon grew in popularity and started selling other products. The company got publicly listed in 1997. Since 2000, they have allowed other businesses to use the portal for selling their own goods. [21]

The original vision of Amazon was to provide an online catalog. Bezos pointed out the dependence on the location, and the costs incurred by that, in case of traditional brick-and-mortar stores, and that is what he intended to eliminate, since technology was getting cheaper, as opposed to real-estate, which kept increasing in price. Albeit this statement by Bezos, during the early days of Amazon, later on, he ended up investing a lot, including in warehouses, to serve the market better. [21] Amazon's key resource is its technological infrastructure, which they built over more than two decades. [22]

Amazon operates with a low profit margin, which makes it attractive to buyers. This is possible thanks to the lack of a physical store and keeping a small inventory. Amazon.com accounts for more than 65% of Amazon's income (23% from third-party sellers) according to data from 2022. Amazon has over 8 million sellers worldwide. From the sellers'

perspective, Amazon's revenue stream consists of advertising fees, which the sellers pay for product promotion, and commission on sales. Another source is Amazon Prime, a subscription-based service for buyers, which guarantees free two-day shipping, access to the video and music streaming catalog and many other benefits. Since Amazon has their own delivery service, it is also a potential source of their profit. Besides the Amazon Marketplace, Amazon also generates income from other services, such as Amazon Web Services (AWS), a cloud provider, Amazon Kindle, an e-reading service, Amazon Advertising and many others. Even though most of their revenue comes from Amazon Marketplace, AWS is Amazon's most profitable service. [22]

### 2.3.3 eBay

In 1995, French-born programmer, Pierre Omidyar founded AuctionWeb, which was rebranded as eBay in 1997. Although initially a portal for individuals selling items to each other directly, today eBay is not only a C2C but also a B2C platform. In 1998, eBay became a publicly traded company. In 2002, eBay acquired PayPal, a popular online payment platform, which they integrated into website as a payment gateway for purchases. The company bought Skype in 2005. [22] In 2007, eBay took a $1.4 billion write-down of Skype, essentially acknowledging that the acquisition did not go as planned, followed by divestment and selling the majority of their stake to an investor group in 2009, then selling their remaining 30% stake to Microsoft in 2011. [23]

Low fees were a key reason behind eBay's success. eBay offered various advantages compared to brick-and-mortar auction houses, e.g., lower commissions and geographic location, thanks to the fact that the site was online, was not a boundary for customers anymore. Besides commission, eBay is profitable thanks to advertising fees, listing fees, final value fees, eBay Plus (a subscription service that provides customers with benefits, such as free shipping) and other revenue streams from its subsidiaries. [24]

Final fees are a significant source of eBay's revenue. The fee can widely vary, depending on the seller's status. Sellers gain better status by selling a larger volume of products and by preserving good reviews. Advertising generates revenue on a per-click basis, if a customer clicks on the promoted ad, the seller gets charged a fee. [24]

### 2.3.4 WooCommerce

WooCommerce (along with Shopify) is one of the most popular ecommerce platforms for building an online store. It is actually a plugin for WordPress, with many integrated tools, developed by Automattic, the same company that owns and operates WordPress. Its popularity can be illustrated by the fact that it has more than 5 million active installations. [25] WooCommerce attracts people with more expertise, as opposed to Shopify, due to its steeper learning curve. The reason why the focus is on WooCommerce instead of Shopify is

due to its open-source, highly customizable nature, and the fact that it can be self-hosted, [26] unlike Shopify. [27]

While WooCommerce can be self-hosted, they do offer hosting solutions, which is one source of their income. Another source is the WooCommerce marketplace, where custom themes and extensions are sold. For shipping, WooCommerce offers a free extension with no fees, with basic functionalities, however they also offer more advanced paid shipping extensions developed by themselves. They also offer their own payment gateway, which has no subscription fee but a fee must be paid after every transaction. [28]

From a security perspective, WooCommerce warns that installing third-party extensions and themes can introduce new vulnerabilities. There are also security related extensions, which can take care of automated backups, provide brute-force attack protection, malware and vulnerability scanning, detailed logging and anti-spam technologies. An SSL certificate is also a basic but inevitable requirement of a secure site, which typically hosting platforms provide for free. WooCommerce also offer software development support for their customers at a paid rate. They also provide a list of trusted developers and agencies that can help with development (possibly another source of their income via commissions). [28]

# 3  System Design

## 3.1  Frontend Website

As suggested by many, I decided to start with the frontend part of the website. I came to this decision for several reasons, namely to discover the functionalities I intend to incorporate in the website, to have a visual idea of what I plan to achieve and also due to the sheer depth of frontend development, I realized this part might take the longest to develop.

### 3.1.1  Chosen Frontend Technologies

Choosing the right technology for a website can be a challenging undertaking. The vast number of technologies competing each other makes it especially difficult for the developers to settle for one. I decided to approach the question more generally than gradually get more specific.

There are many frontend frameworks out there in the market, such as React, Vue.js, Next.js, Svelte, etc. According to StackOverflow trends, React is the most popular framework, followed by Angular and Next.js. [29] Google Trends outlines similar statistics. [29] Since I have experience in Angular, I chose this framework for my website. The strongly typed nature of TypeScript helps with building more stable apps, with the slight disadvantage of the need for compilation.

Once I selected the framework, I looked for a UI component library. After some research, I narrowed down the potentials to 3 libraries: PrimeNG, Angular Material and Taiga UI. Due to my work, I have experience with Angular Material, however I am not too satisfied with its appearance, since it tends to give the website looks akin to Google products. Taiga UI seemed quite promising; however, it is still in an earlier stage of its development and has a smaller userbase, which also means less documentation. With PrimeNG, I had some experience, thanks to personal projects and also work. PrimeNG offers the widest range of components and although there are reports of occasional bugs with some components, I decided to choose this framework, since it is easy to use and visually appealing.

For styling, I contemplated using Tailwind, since it allows rapid development speed, however it also has its own learning curve and I figured that without a strong CSS background, Tailwind may actually cause more problems than it solves. For this reason, I decided to proceed with the project using pure CSS and potentially PrimeFlex, since it is a utility library optimized for PrimeNG.

## 3.2  Wireframes

Once settled with the frontend technologies, I decided to create a blueprint of the website I was imagining. Wireframes seemed perfect for this purpose. I decided to use Figma, since I

had experience with it from before and it is an easy-to-use tool for designing. I created the design of different pages, namely the home page, the page of a subcategory, the page of a product and the page of the items added to the cart. Some constant elements include the header and the footer, which are displayed on all pages.
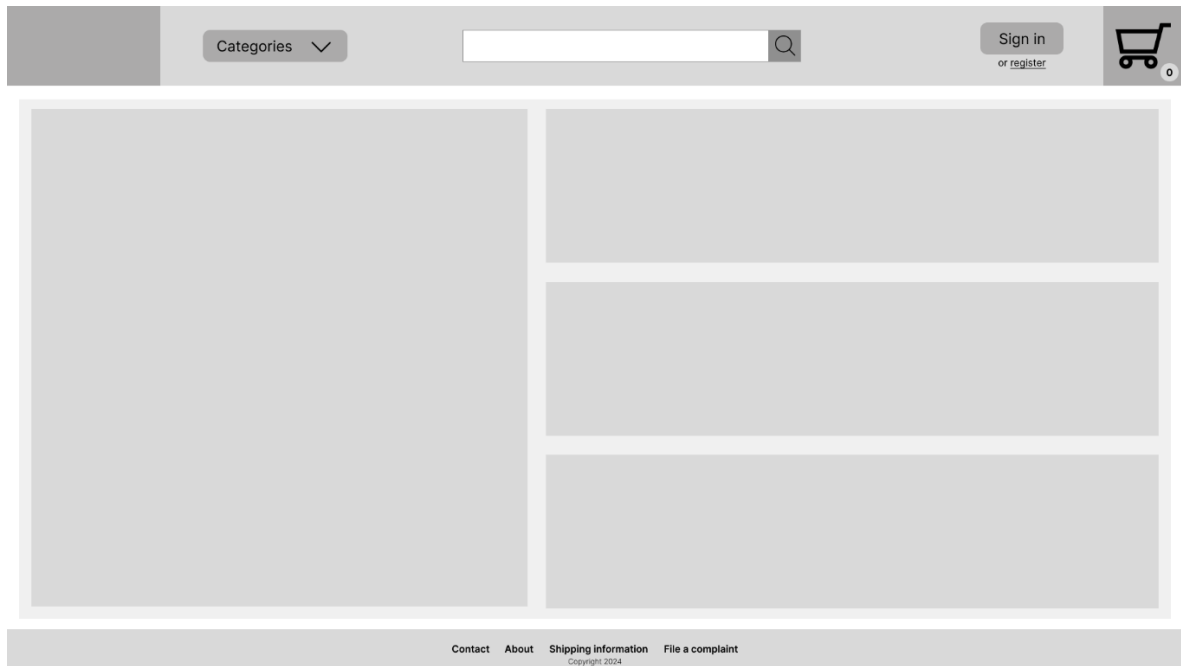
**Figure 3.1 - Home page**

Figure 3.1 - Home page depicts the home page of the website, which includes some promotions, the header and the footer. The header includes the site id (the logo of the website with a link to the home page), a multi-level dropdown for selecting the appropriate category and subcategory, a search field for looking up products, sign in and register buttons and the user's cart. The footer includes the most typical links for an online store, such as contact, the about page, shipping information and a page for handling complaints.
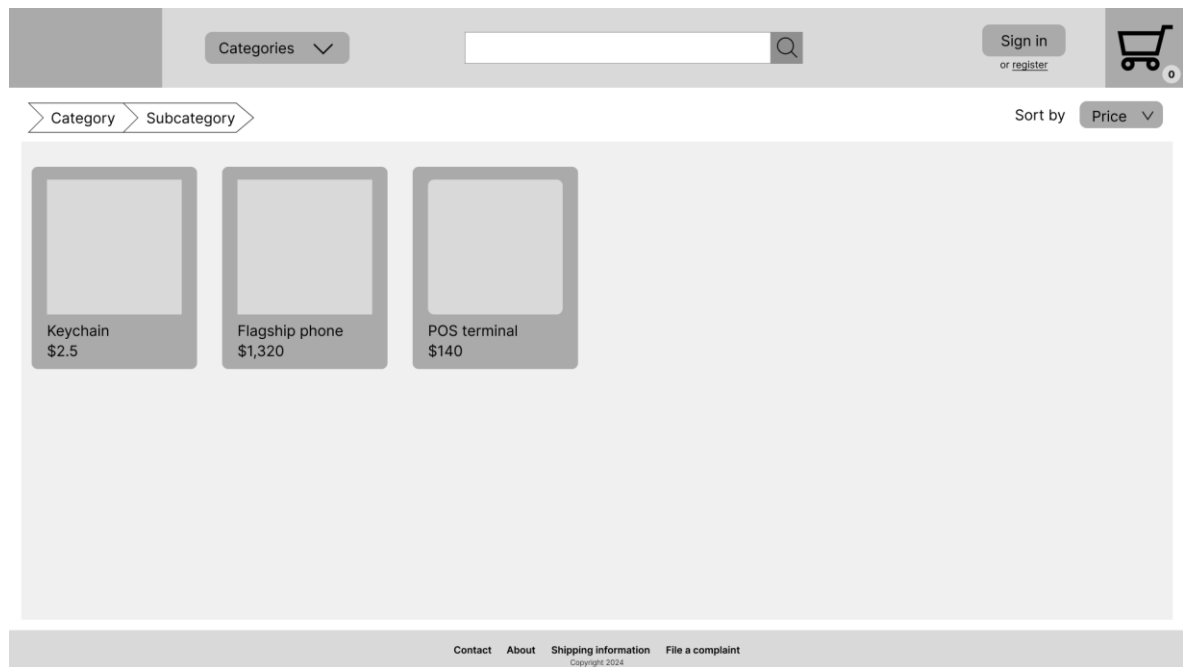
**Figure 3.2 - Subcategory Page**

Figure 3.2 - Subcategory Page includes breadcrumbs, that show which category and subcategory the user selected, product cards with the names and the prices of the products on them.
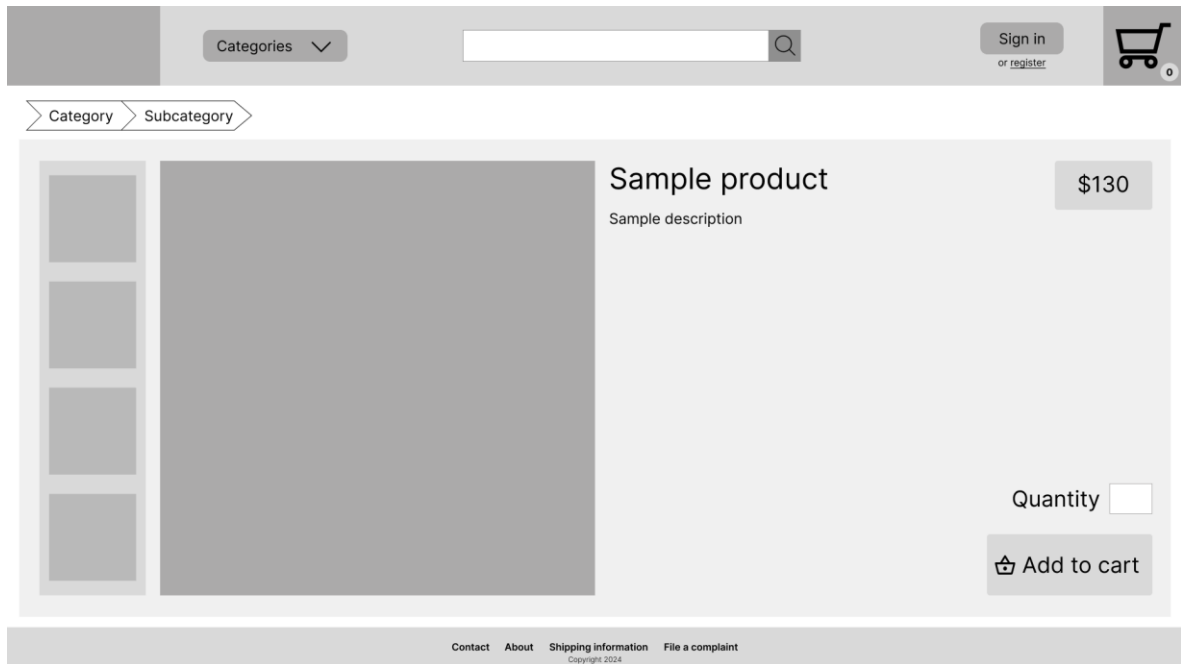
**Figure 3.3 – Product Page**

Figure 3.3 – Product Page shows images of the product, along with a photo carousel, name and description of the product, the price of it, the quantity to order (which defaults to 1) and a button to add the required quantity to the cart. It also includes the breadcrumbs that show the category and the subcategory of the product.
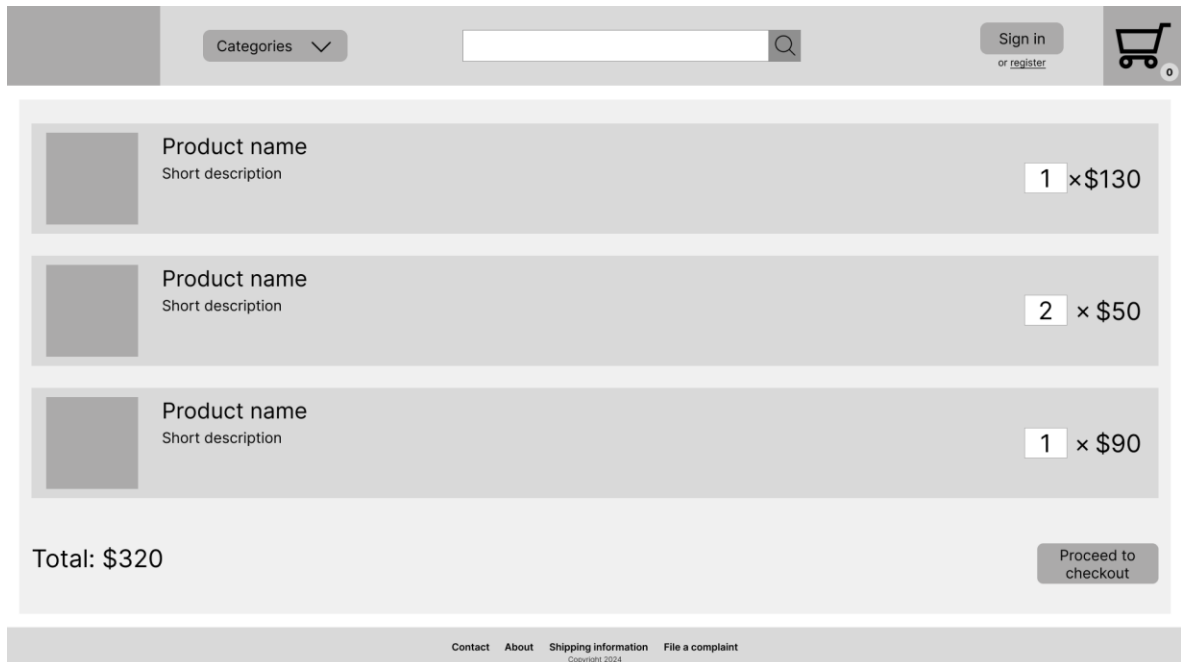
**Figure 3.4 - Cart Page**

Figure 3.4 - Cart Page shows the items that the user has added to the cart. A thumbnail is shown of the item, along with its name, a short description, the price and the quantity the user specified and a proceed to checkout button, which once clicked takes the user to the page where they are prompted for their personal information and shipping address.

# Bibliography

[1]  D. N. B. Gajjar, "Commerce, E-Commerce and Trade," *International Journal for Research in Management and Pharmacy (IJRMP),* vol. 2, no. 1, 2013.

[2]  V. K. Yadav, "Global Prospect of E-commerce," *International Journal of Social Science & Interdisciplinary Research,* vol. 3, no. 1, 2014.

[3]  Y. Tian, History of E-Commerce, 2007.

[4]  K. Nguyen, Technology Contribution in Electronic Commerce, 2019.

[5]  D. Zhe, E-commerce trend and E-customer analyzing, 2017.

[6]  V. Simakov, "History of Formation of E-commerce Enterprises as Subjects of Innovative Entrepreneurship," *Three Seas Economic Journal,* vol. 1, no. 1, 2020.

[7]  S. Krug, Don't Make Me Think, Revisited, New Riders, 2014.

[8]  M. S. S. Padmannavar, "A Review on Ecommerce Security," *International Journal of Engineering Research and Applications (IJERA),* vol. 1, no. 4, pp. 1323-1327.

[9]  M. D. Kalamkar, "A study of Ecommerce Security," *IJCTA,* vol. 10, no. 9, 2017.

[10] D. M. A. Hussain, "A Study of Information Security in E- Commerce," *International Journal of Computer Engineering Science,* vol. 3, no. 3, 2013.

[11] Y. Sun, J. Zhang, Y. Xiong and G. Zhu, "Data Security and Privacy in Cloud Computing," *International Journal of Distributed Sensor Networks,* 2014.

[12] P. Yang, N. Xiong and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," *IEEE Access,* vol. 8, pp. 131723-131740, 2020.

[13] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," in *International Conference on Computer Science and Electronics Engineering*, 2012.

[14] M. I. Al Ladan, "E-Commerce Security Challenges: A Taxonomy," *Journal of Economics, Business and Management,* vol. 4, no. 10, 2016.

[15] IBM Cloud Education, "Object vs. File vs. Block Storage: What's the Difference?," [Online]. Available: https://www.ibm.com/blog/object-vs-file-vs-block-storage/. [Accessed 6 May 2024].

[16] K. Zeng, "Provable data integrity verifying method, apparatuses and system". Patent US20090171878A1, 2008.

[17] KraneShares, "Alibaba 101: An Overview of the World's Largest E-Commerce Company," 2014. [Online]. Available: https://kraneshares.com/resources/2014_12_alibaba_overview.pdf. [Accessed 7 May 2024].

[18] Alibaba, "Alibaba Pricing," [Online]. Available: https://seller.alibaba.com/pricing. [Accessed 7 May 2024].

[19] BBC, "Alibaba: What exactly does it do?," 4 September 2014. [Online]. Available: https://www.bbc.com/news/business-29077495. [Accessed 7 May 2024].

[20] Alibaba, "Alibaba.com sourcing guide," [Online]. Available: https://www.alibaba-na.com/hubfs/ustradeshows/supplements_nutrition/alibaba_com_sourcing_guide.pdf. [Accessed 8 May 2024].

[21] N. Maio and B. Re, "How Amazon's E-Commerce Works?," *International Journal of Technology for Business,* vol. 2, no. 1, 2020.

[22] D. Pereira, "Amazon Business Model," Business Model Analyst, [Online]. Available: https://businessmodelanalyst.com/amazon-business-model/. [Accessed 9 May 2024].

[23] eBay Inc. Staff, "eBay Inc. Reiterates 'The Truth About Skype'," eBay, 3 May 2014. [Online]. Available: https://www.ebayinc.com/stories/news/ebay-inc-reiterates-truth-about-skype/. [Accessed 9 May 2024].

[24] D. Pereira, "eBay Business Model," Business Model Analyst, 2023. [Online]. Available: https://businessmodelanalyst.com/ebay-business-model/. [Accessed 9 May 2024].

[25] Automattic, "WooCommerce," Automattic, [Online]. Available: https://wordpress.org/plugins/woocommerce/. [Accessed 8 May 2024].

[26] S. Trovato and R. Watts, "WooCommerce Vs. Shopify (2024 Comparison)," Forbes, 2024. [Online]. Available:

https://www.forbes.com/advisor/business/software/woocommerce-vs-shopify/. [Accessed 8 May 2024].

[27] T. Wingfield, "Can I Host Shopify On My Own Server?," Kanteneo, [Online]. Available: https://kanteneo.com/blog/can-i-host-shopify-on-my-own-server/. [Accessed 8 May 2024].

[28] K. Marr, "WooCommerce pricing: How much does it cost to run a store?," WooCommerce, [Online]. Available: https://woocommerce.com/posts/woocommerce-pricing/. [Accessed 8 May 2024].