C2C Application as an Example of E-shop for Handmade: Tools, Security Issues, Basic Technologies

Valentyna Pleskach [1,2], Viacheslav Zosimov [1], Oleksandra Bulgakova [1], Mariia Pleskach [2] and Eva Volnyanska [1]

[1] *Taras Shevchenko National University of Kyiv, Bohdan Hawrylyshyn str. 24, Kyiv, 04116, Ukraine*
[2] *Vilnius Gediminas Technical University Saulėtekio al. 11, Vilnius, LT-10223, Lithuania*

Abstract

The paper is devoted to the analysis of the economic state and level of development of the digital economy and e-commerce, as the main component of the digital economy. The paper presents the C2C application of e-shop for handmade. In this article was determining legal regulation of e-commerce, innovations in this area, security issues, new technologies of building of online shopping website for handicraft. This problem was solved by using the architecture of the designed system, developed according to the type of three-tier client-server architecture. It gives many individuals and small business owners a low-cost way to sell their goods and services. Problems of personal data protection were also considered.

Keywords [1]

E-commerce; C2C application, legal regulations for e-commerce, e-shop for handmade, security of e-commerce systems

1. Introduction

Digital era of web 4 - it is known as Symbiotic and web 5 is coming in the very near future, can be considered as a decentralized Symbionet Web. The future of e-commerce and the Semantic Web is dependent on how far the relevant information technology advances. These include the developments in the global grid, new collaboration technologies, and penetrating computing.

E-commerce is a branch of the digital economy that represents commercial and monetary transactions and their business processes that take place using computer networks [1]. E-commerce refers to using the Internet and intranets to purchase, sell, transport, or trade data, goods, or services. E-trade is an integral part of the digital economy. It provides the organization with a number of advantages over ordinary physical representative offices, such as: quick information transactions, which is especially relevant for foreign operations; reduction of costs not related to production; shorter sales cycle; costs for information exchange are significantly reduced due to the use of cheaper telecommunication methods; greater openness of enterprises to users [2-3].

Consumer-to-consumer (C2C, C2B) e-commerce, which is called peer-to-peer (P2P) e-commerce, refers to electronic transactions completed between and among individuals. These transactions can also include intermediaries, such as olx platforms or social network sites that organize, manage, and facilitate the C2C networks. C2C activities may include transactions resulting from classified music, career, job matching, personal matchmaking services, handmade, etc. One advantage of C2C of e-commerce is that it reduces the administrative and commission costs for both buyers and sellers. It also gives many individuals and small business owners a low-cost way to sell their goods and services.

According to the Global Payments Report, employment in the e-commerce sector increased by 80% from 1997 to 2016 years [4]. The global e-commerce market was predicted to grow by $100.63 billion from 2020 to 2024 years [5]. And the total retail revenue from e-commerce will reach $6.54 trillion.

until 2023 year [6]. It was also expected that by 2040 year, 95% of all purchases will be made through e-commerce [7]. But the conditions of 2021 year and war state had a significant impact on the development of e-commerce. The COVID-19 pandemic has greatly motivated customers around the world to shop from home. The business responded to the potential customers desire to visit supermarkets, shopping centers and offline stores as rarely as possible, therefore the business urgently updated and expanded the capabilities of online stores and logistics. Companies that did not have time to digitize in a timely and qualitative manner or had too many "problem areas" in their work before the onset of the COVID-19 left the market. According to Deloitte Ukraine survey data, on the eve of the war state, an important trend was observed for the second year in a row: a two-fold predominance of growth rates online over offline [8].

The 22% of respondents indicated that they started to buy more often online, and only 9% shop more often offline. And this trend only intensified. As the research of Soul Partners and Baker Tilly Ukraine showed, the sales of the e-commerce market in 2020 year increased by 41% and reached $4 billion, which was 8.8% of the total volume of retail trade in Ukraine. This share was expected to be at the level of 9.2% or $4.4 billion by the end of 2021 [9]. After three months of the 2022 year war state, Promodo experts analyzed how key indicators changed in seven segments of Ukrainian e-commerce from February to May. Indicators paid attention to: advertising budget, income, users, customer acquisition cost, average check, part of advertising costs. So, at the beginning of March, e-commerce almost "died". Already on the day of the invasion, all online stores lost an average of 82.7% of sessions [9]. In the first week, Ukrainian online retailers lost almost all of their income. On average, it fell by 92%. But already in the middle of March, incomes began to grow along with a significant increase in the number of sessions. At the end of May, some categories even returned to pre-war state indicators (pet products and cosmetics together with household and hygiene products) [10]. The fact is that the war changed not only the place of stay of many Ukrainians, but also the patterns of their shopping behavior [10]. In a new place, people cannot always find the necessary goods, so they began to order them online more often. The need to arrange life in a new place caused a temporary increase in purchases.

It is at such a time that the issue of organizing work with user data, methods of ensuring transaction security and protecting confidential user data within the e-trade system becomes quite relevant.

2. Legal regulation of e-commerce

Important problem is legal regulation of e-commerce

With the emergence of e-commerce in the international economic space, along with its advantages, real and potential risks also appeared, which regulatory and legal acts in the field of e-commerce are designed to regulate.

- Among the main challenges faced by e-business entities are:
- Users Identification to ensure the safety of financial transactions;
- Privacy and protection of consumers personal data ;
- Taxation of electronic business entities;
- Intellectual property protection;
- Content control that is difficult to follow on the Internet;
- Disputes settlement and protection of the parties' rights to the conflict.

At the moment, there is no single unified set of laws in the field of e-commerce in the world, so every country in the world bears personal responsibility for the development of its own regulations. The state of adoption of regulatory legal acts on e-commerce in the world and in each country can be tracked using the resource of the United Nations Commission on Trade and Development. This is the world's first e-map that tracks the state of e-commerce legislation in the areas of e-transactions, consumer protection, data protection/privacy and cybercrime legislation across the 194 UNCTAD (United Nations Commission on Trade and Development) member countries. It indicates whether this or that country has adopted legislation or has a bill pending adoption [11].

In Ukraine, entrepreneurial activity in the field of electronic commerce did not fall under the jurisdiction of a separate law until September 3, 2015, when a separate Law "On E- Commerce" was established. Before that, all controversial issues, such as the relationship between online stores, services and users, were resolved in accordance with the principles laid down by the Civil Code of Ukraine and

the Law of Ukraine "On the Protection of Consumer Rights". The law was amended several times during 2017-2020 and is currently published in the version dated 04.19.2020 [11-12].

Now need to know such as key e-commerce Laws – taxes, payment gateways, trademarks, patents and copyrights, shipping restrictions, inventory, age restrictions, business insurance, licenses and permits, PCI compliance, customer privacy. Legal regulations for e-commerce are well described in site https://single-market-economy.ec.europa.eu/sectors/tourism/business-portal/understanding-legislation/legal-regulations-e-commerce_en.

3. Innovations in e-commerce

In order to compete qualitatively in the e-commerce market, the leaders of this industry invest in innovations in this industry, which not only facilitate work, but also increase interaction with consumers.

Interaction methods with consumers:

- With the development of the e-market, classic B2B and B2C models are declining in popularity. Instead, business prefers a new trend - D2C (Direct-to-Consumer). This method consists in the fact that manufacturers abandon middlemen, marketplaces, etc., in favor of direct sales of goods to their target auditory;

- Application of the "white label" principle, which means applying your name and brand to the product purchased from the distributor. In this way, the entrepreneur invests not in the creation of the product, but in its marketing, design and application of advanced technologies.

Payment methods:

- Along with traditional payment methods such as credit cards, bank transfers, e-wallets, etc., currently a very small number of people pay with Bitcoin or other cryptocurrency, about 1% of users [13]. However, cryptocurrencies, especially Bitcoin, have several advantages for online store owners, such as low transaction fees and no reverse transactions. Perhaps this service will lead to more e-commerce businesses accepting cryptocurrencies for transactions in the near future.

- Payment methods using a QR code are becoming very popular [14]. This methods are expected to be widely used in the near future, especially in growing markets, primarily because it is inexpensive to implement and easy to use. This payment methods are already in use, however, modern QR code payment solutions require special applications that allow them to be used only in one institution. Mature markets are actively using popular digital wallets built in consumer smartphones, such as Apple Pay, Samsung Pay and Google Pay, which is making QR code payments more accessible.

- Application of artificial intelligence (AI) in the field of payments. Text-to-speech functions or speech-to-text chatbots are becoming much more accessible in this field, which will become an important aspect of digital transformation in the field of in-app payments. Digital banking applications that offer this feature enable customers to initiate invoice payments and transactions via voice commands [15].

4. Online shopping security

Problems arising during online ordering can be both from the side of online store owners and from the side of e-business users.

4.1. Problems faced by e-business owners

Consider the complexities that can affect the convenience of providing an online purchase (from the point of e-business owners view):

1. User identification in the system.

When a visitor registers on an e-commerce website, the information they enter may be incorrect, which can lead to further problems. For example, COD purchases made with an invalid phone number

and address can result in significant lost revenue. Therefore, it is important to conduct an online background check for each potential client.

2. Cybersecurity in the system.

Cyber attacks can undermine the security of an e-commerce website, infect it with viruses, or even compromise the security of registered customer data. Attackers can potentially gain access to sensitive data, including credit card details. This scenario is one of the biggest problems to overcome in an e-commerce business and it is certainly one of the biggest problems every e-commerce owner faces.

3. The "abandoned shopping cart" problem.

A difficult problem that e-commerce businesses face is shopping cart abandonment. Statistics show that online shoppers abandon their shopping carts 68% of the time [16], and some stores can experience abandonment rates as high as 80% [7].

4. Product return and refund policy.

Over 60% of online shoppers look at a store's return policy before making a purchase [10]. The 48% of customers would buy more if stores offered less complicated refunds, and inconvenient return policies cause 80% of customers to abandon a purchase from that store [16]. For e-commerce businesses, the challenge is how to provide convenient returns and refunds to the customer while not incurring business losses.

5. Security of shopping channels.

According to statistics, customers who interact with the service using several channels spend three times more in the store than users of one channel [16]. Setting up an e-commerce system requires significant optimization, taking into account the technical side of implementation, as well as the areas of marketing, content customization, and user service quality.

4.2. Security of e-commerce systems

Creating an online store for conducting e-commerce is more than just the process of selling products over the Internet. E-commerce websites need advanced security systems, as cybercrimes such as identity theft are among the most common crimes committed against consumers. Moreover, the majority of cyberattacks are carried out specifically in the direction of small business electronic stores.

4.2.1. Personal data protection

To ensure the security of e-commerce system, should use several e-commerce website protection tools, such as:

1. Using multi-factor authentication: After the user enters the login information, he will instantly receive an SMS or email with further actions. This move limits the scammers as they need more than just logins and passwords to access legitimate user accounts.

2. Secure Sockets Layer (SSL) certificates: One of the main benefits of SSL certificates is the encryption of confidential data transmitted over the Internet. This is a very important step because all the data sent will pass through several computers before the destination server receives it. If SSL certificate encryption is missing, any electronic device between the sender and the server can access sensitive data. In this way, hackers can take advantage of exposed passwords, usernames, credit card numbers and other information. An SSL certificate is designed to make data unreadable by third-party users.

3. Use of firewalls: Firewalls must protect the server against spam, XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery), malware, SQL injection and other web attacks -site. This ensures that the traffic that accesses the e-commerce store consists of only real users [17].

In addition to the technical methods of personal data protection listed above, legal measures also play an important role. Thus, e-commerce platforms must ensure and bear responsibility for the safety (protection) of consumer data obtained when concluding a relevant contract (public contract), including an electronic one. It should be noted, that personal data of consumers can be processed, including through profiling, for the purpose of providing the ordered goods or services, ensuring the fulfillment of obligations under the contract and under the condition of: having the unequivocal, prior, recorded

consent of the consumer; on the basis of the contract, in the part of the data, the processing of which is necessary to provide the service ordered by the consumer.

Unfortunately, now, in accordance with Part 3 of Art. 14 of the Law of Ukraine "On Electronic Commerce", the registration of a person in the information system of an e-commerce entity means giving consent to the use and processing of his personal data and taking other actions provided for by the Law of Ukraine " On the Protection of Personal Data". That is, the registration of a user in a certain system implies the automatic granting of his consent to the processing of personal data, even without marking that he gives such consent.

At the same time, according to Art. 2 of the Law of Ukraine "On the Protection of Personal Data", in the field of e-commerce, the consent of the subject of personal data may be given during registration in the information and telecommunications system of the subject of e-commerce by putting a mark on granting permission to process his personal data in accordance with the formulated the purpose of their processing, provided that such a system does not create opportunities for the processing of personal data until the moment of ticking. That is, Art. 14 of the Law of Ukraine " On Electronic Commerce" requires coordination with the branch Law of Ukraine "On Protection of Personal Data", with the aim of bringing the activities of digital services to the legislation regulating the protection of personal data and reducing cases of violation of the informational rights of users of such services [21].

It should be noted, that the terms of the Agreement on the provision of certain services should not oblige the consumer to give consent to the processing of data that is not necessary for the provision of the services ordered by him, as well as to provide for the processing and/or transfer by third parties of personal data and other data of the consumer for the purpose of providing other services than those provided for in the subject of the Agreement or additional services that the consumer did not order. The composition and content of the consumer's personal data that will be collected and processed during the provision of the service (services), the purposes and duration of their processing, the possibility and method of withdrawing consent to their processing at any time must be determined by the contract for the provision of services and must be appropriate, adequate and not excessive in relation to the purpose of their processing.

It is extremely important to give the consumer the right to exercise his right to withdraw his consent to the processing of personal data and other consumer data at any time, i.e. the opportunity to fully exercise the "right to be forgotten". Due to the absence of a mandatory provision in the regulatory and legal acts of Ukraine that the procedure for withdrawing consent to the processing of personal data should be as simple as obtaining it, the user of some digital services is deprived of the right to delete personal data about himself and to independently manage his personal account (profile). In this regard, it is necessary to implement the rule that any digital service (regardless of the type: online store, e-mail, gaming business website, etc.) must necessarily contain a technical possibility for the user in any when to delete a personal account, profile or withdraw consent to the processing of personal data. That is, the "right to be forgotten" should be provided, including by automated means using electronic communication networks.

4.2.2. Transaction security

In the context of protecting credit card data, it is important to follow the standards and protection recommendations proposed by the Payment Card Industry Security Standards Council (PCI SSC) [18]. It emphasizes the absolute importance of destroying customer data as soon as a transaction is complete. In addition, the PCI SSC absolutely insists that no cardholder information is ever stored on the system's servers. It is worth remembering that if there is nothing to steal in the system, it will not be at risk.

The main measures to ensure the security of payment data are:
- Encryption is a very effective and practical way to protect data transmitted over the network. The sender of the information encrypts the data using a secret code, and only the specified recipient can decrypt the data using the same or a different secret code;
- Digital signature ensures the authenticity of information. A digital signature is an electronic signature certified by encryption and a password;
- Security certificates such as SSL/TLS (Transport Layer Security) not only reduce the risk of security breaches, but also provide a foundation for legal proceedings in the event of a breach.

4.2.3. Blockchain technologies

Blockchain or distributed ledger technology (DLT - Distributed Ledger Technology) assumes that data is structured in blocks, and each block copies information about a transaction or a batch of transactions. Each new block is connected to other blocks in a cryptographic chain in such a way that it is almost impossible to break into this system and steal or replace information there. All transactions within blocks are verified and agreed between blocks by a consensus mechanism, ensuring that each transaction is true and correct.

Thus, blockchain technology provides decentralization of information involving blocks in a distributed network where a single user cannot change the transaction record. This technology is extremely useful in the field of e-commerce, but has certain security nuances and needs further research.

5. Ways of cyber protection on a real example

An online store selling handmade goods was created to test the technology of intelligent interface customization.

5.1. Online store description

Several types of UML diagrams will be schematically depicted below, each of which models the subject area from different perspectives. The online handmade goods store is the main object of the simulation, so all diagrams will be created based on the main component.

Figure 1 show a diagram of the options for using the developed web resource. The web resource was created according to the classical online stores scheme and has all the necessary functionality: a catalog, a shopping cart, an online order, an authorization system.
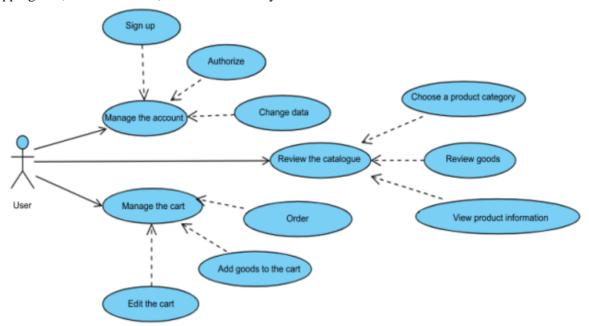

Figure 1: UML-diagram of precedents (options of use)

Figure 2 show the UML class diagram that formed the basis for creating a web resource. It contains classes: Catalog, Category, Product, Website, User, Order. Figure 3 show the sequence of user actions from the moment he entered the site and until the order acceptation. At the top of the diagram, the roles of users are indicated: Client, Administrator, as well as functional modules which the client interacts with: Product catalog, Cart. After entering the site, the client interacts with the product catalog. The result is the added to the necessary products. At the stage of the client interaction with the Cart module,

the order is placed. At the final stage, the Administrator who carries out the final confirmation of the order is included in the scheme.
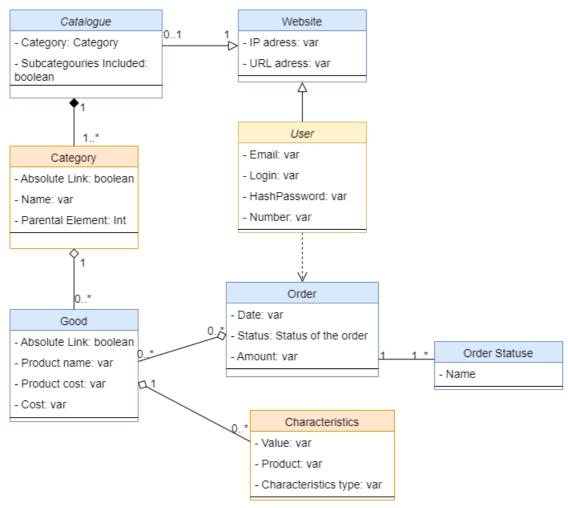

Figure 2: UML class diagram

5.2.   Architectural solutions for e-commerce software system

The designed system is an example of a three-level type of client-server architecture [19-20]. A feature of this type of architecture is the presence of middleware between the client machine and the data server. All data logic and business logic is stored within the middleware. The use of middleware increases the flexibility and productivity of the developed system. The three-tier architecture is divided into 3 layers, such as the presentation (client) layer, the application (business logic) layer, and the database layer (data layer), which can be seen in the system deployment diagram (Figure 4).

The deployment system diagram shows the architecture of the designed system, developed according to the type of three-tier client-server architecture. The client machine, which is processed by the presentation level, is schematically represented by blocks Client x_1-x_n. By connecting via a private network, the system client gets access to the central (intermediate) level of the application. The central element of the developed client-server architecture is the web server, which is a high-performance computer system that can host several web resources.

Also, as an additional third-party component of the movement and data transfer of the e-commerce system, it was decided to depict the payment system on the diagram, which is referred to by the program for carrying out client transactions. Its component, the payment gateway, is used by the software system to transfer bank data of users using a secure connection with the SSL protocol.

The design pattern of the project system was based on the principles of the MVC (Model View Controller) model, which assumes that the application consists of a data model, information about the

154

external interface, and information about logic management. The template assumes that each of these elements has been separated into different objects. MVC is an architectural pattern that mostly deals with the user interface and application interaction layer.

As a result of this type of design, we get a layered and tiered system structure that, while bulky, is justified because it provides a way to easily modify and reuse application modules.
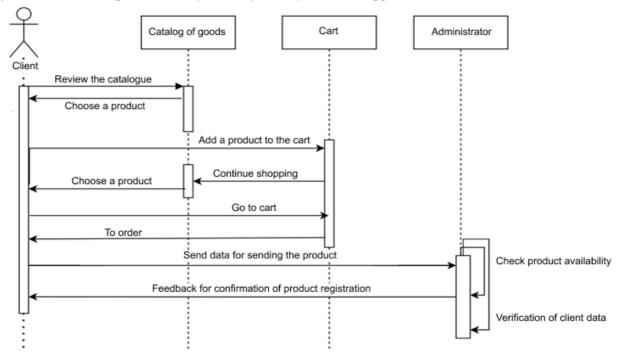

Figure 3: UML sequence diagram without registration and authorization
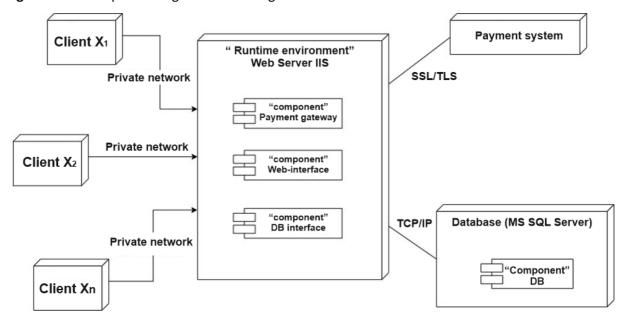

Figure 4: System deployment diagram

5.3. System application server architecture

The system architecture is an implementation of the ASP.NET MVC 5 technology. It enables a high-performance development model and facilitates the writing of clear and structured code architecture, supporting development through testing and easy system scalability. The latest version of the MVC 5 development technology introduces a new user authorization technology based on the ASP.NET

Identity system using OWIN and Katana components instead of the Simple Membership Provider. MVC 5 technology also offers the function of debugging and overriding authentication filters. MVC 5 technology is used in this work in combination with additional extensions such as Web API, Entity Framework (Code First), ASP.Net Identity, ASP.NET Cache.

The designed system is divided into separate modules that are responsible for their sphere of responsibilities and refer to each other for interaction. The present modules are responsible for communication with the web server and database, implement data models, and contain classes for encrypting confidential resource data. A connected extension that performs the IsSelected function, which implements the projection of product items of the resource onto the site pages. The implementation of this function occurs from the markup components located in the View model elements, in particular, _FrontLayout.cshtml. Work in the system occurs due to the interaction of system components and at the time of transfer of requests from one component to another. The work is focused on several basic elements of the system: electronic store module, database, user entity, product, payment module. The requests between these modules and the responses they send to each other are depicted in the system sequence diagram (Figure 5). The diagram shows the sequence of requests coming from the user's web server to the system and the responses that the system sends to the client.
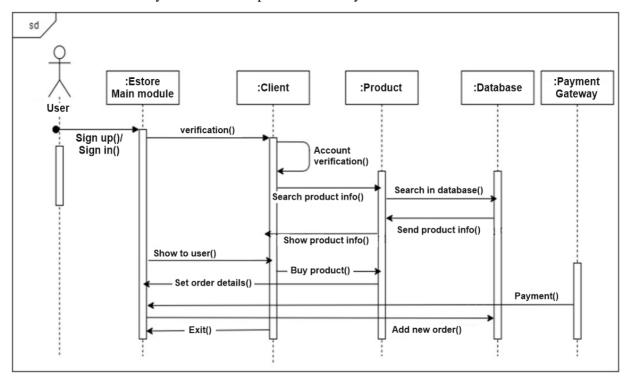

Figure 5: System sequence diagram

The processing of requests begins with the main module of the system, which is an interface of interaction with the client, on which he sees all the information. The sequence in the diagram is left to right and top to bottom. The beginning of the sequence is the client's request to the system.

The sequence diagram show the main entities of the project: the user, the main module, the client, the product, the database and the payment system and the relationships between them. The main module transfers the processing queue to the client module, which is responsible for user identification. After that, the main functionality of product search and selection, ordering and payment processing is implemented, which is the responsibility of separate relevant modules of the system.

5.4. Protection of users' personal data

Protection of personal data of users of the resource for the sale of handmade products is ensured by encryption of confidential data using a closed (private) key [22]. This method is a secure method of storing data such as customer passwords, bank details, etc. "Privacy" of the key ensures that the key is

stored on the server and cannot be published or shared with third parties. Also, in order to guarantee that the data has not been modified during transmission and is really true, hashing is carried out using "salt", which provides additional protection when processing personal data.

When the user is authorized, the password provided is applied by a hash function and the result is compared with the one stored on the server. Thus, the system ensures that, firstly, the data stored on the server cannot be stolen and read by third parties and, secondly, user authorization takes place in a reliable manner. User passwords are hashed for storage in the database by salting the raw password using the SH1 algorithm. The process of user authorization and his access to the system module is depicted in the system interaction diagram (Figure 6).
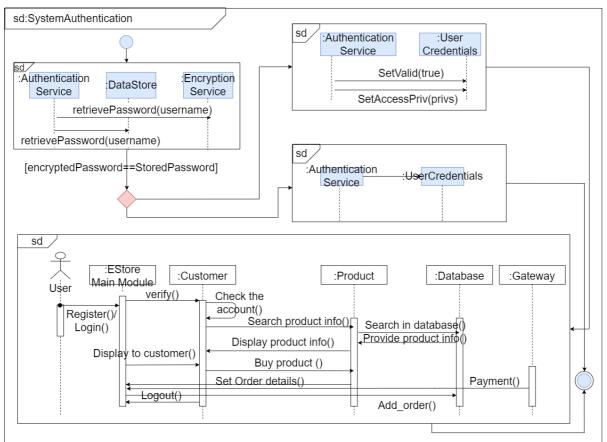

Figure 6: System interaction diagram

The interaction diagram depicts the process when the user gets to the login point of the authentication service, provides his login data, which is compared by the encryption service with the data stored by the system. If the provided data is incorrect, the client is directed to the exit point of the system. In the case of valid data, the user is directed to the main module of the software system, where his interaction is worked out according to the scheme of the sequence diagram

6. Conclusions

The paper researched the economic state and level of development of the digital economy and e-commerce, as the main component of the digital economy, in Ukraine and the world; analyzed regulatory and legal aspects of conducting electronic business activities, modern approaches to conducting trade activities on the Internet; development prospects, trends and problems of electronic commerce; online payment methods at the global business level and within Ukraine; considered cyber protection systems both at the level of online store owners and at the level of buyers. The application of the principles of security organization and protection of personal data in the system was shown on a real example of C2C application of e-shop for handmade.

7. References

[1] V. Pleskach, V. Krasnoshchok, M. Melnyk, S. Klymenko, R. Tumasonis Current State and Trends in the Development of E-Commerce Software Protection Systems. CEUR Workshop Proceedings , 2021, 3179, pp. 79–88

[2] Retail e-commerce sales worldwide, 2022. URL: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

[3] G. Sreedhar, Improving e-commerce web application through business intelligence techniques. N.Y.: IGI Global, 2018. P. 357

[4] A study of 46000 shoppers shows that omnichannel retailing works, URL: https://hbr.org/2017/01/a-study-of-46000-shoppers-shows-that-omnichannel-retailing-works

[5] Why are shoppers leaving my site, URL: https://tinuiti.com/blog/ecommerce/why-are-shoppers-leaving-my-site/

[6] Cart abandonment rate statistics, URL: https://www.barilliance.com/cart-abandonment-rate-statistics/.

[7] Estimated worldwide mobile e-commerce sales URL: https://www.statista.com/chart/13139/estimated-worldwide-mobile-e-commerce-sales/.

[8] Inside Kimberly Clarks digital strategy, URL: https://digiday.com/marketing/inside-kimberly-clarks-digital-strategy/?_ga=2.251620550.1340709069.1599739754-637882819.1599739754.

[9] The e-commerce market in Ukraine has reached $4 billion, URL: https://soulpartners.com.ua/en/news/tpost/casugamy91-the-e-commerce-market-in-ukraine-has-rea

[10] How the ukrainian ecommerce changed during a month of the war, URL: https://www.promodo.com/blog/how-the-ukrainian-ecommerce-changed-during-a-month-of-the-war/

[11] UNCTAD (United Nations Commission on Trade and Development) URL: https://unctad.org/

[12] M. Pleskach, V. Krasnoshchok, O. Orliuk, V. Pleskach, Y. Melnyk, Mechanisms for Encrypting Big Unstructured Data. Technical and Legal Aspects 2021 11-th International Conference on Advanced Computer Information Technologies, ACIT 2021, Proceedings, 2021, pp. 504–509.

[13] Z. H. Wu. Cloud Computing: Analysis of the Core Technology. Posts & Telecom Press, 2011, URL: http://www.esri.com/news/arcwatch/0110/feature.html.

[14] Ranking Db-engines, URL: https://db-engines.com/en/ranking.

[15] Maintaining payment security, URL: https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security.

[16] Personalized product recommendations in ecommerce, URL: https://www.perzonalization.com/blog/personalized-product-recommendations-in-ecommerce/.

[17] V. Zosimov, O. Bulgakova, P. Popravkin, V.Mashkov, Risk of Information Loss Using JWT Token, CEUR Workshop Proceedings, 2021, 3101, pp. 292–299.

[18] Payment Card Industry Security Standards Council (PCI SSC), URL: https://www.pcisecuritystandards.org/.

[19] V. Zosimov, O. Bulgakova, V. Pozdeev, Semantic Profile of Corporate Web Resources. CEUR Workshop Proceedings, 2021, 3179. pp. 389–397.

[20] V. Zosimov, O. Bulgakova, Web Data Displaying Approach Based on User's Semantic Profile Templates. International Scientific and Technical Conference on Computer Sciences and Information Technologies, 2020, 1, pp. 428–431 doi:10.1109/csit49958.2020.9321839.

[21] http://baltijapublishing.lv/omp/index.php/bp/catalog/view/58/1058/2317-1

[22] E. Turban, D. King, J. Kyu Lee,T. Liang, D. C. Turban Electronic Commerce A Managerial and Social Networks Perspective. Eighth Edition. Springer International Publishing Switzerland, 2015, 791 p. doi 10.1007/978-3-319-10091-3.