Journal of Education and Practice
ISSN 2222-1735 (Paper) ISSN 2222-288X (Online)
Vol.12, No.3, 2021 www.iiste.org

Electronic Payment Systems – Payment Gateways and Data Security Standards

Lorraine Jonassen[1] Binh Tran[1*] Hyesung Park[1] Karen Benson[1]

1. School of Science and Technology, Georgia Gwinnett College, Lawrenceville, GA 30043, USA

* E-mail of the corresponding author: btran5@ggc.edu

Abstract

The use of mobile applications has allowed electronic transactions to be made anytime, anywhere, and by anyone. The Internet has made it possible for businesses to expand their reach across the globe. As a guiding agent for purchasing decisions, social media's proliferation has expanded businesses' ability to generate revenue [1]. In short, e-commerce has become a mainstay in the way consumers shop.

The findings related to this study are three-fold. First, a systematic and rigorous approach is applied to research the importance of Payment Gateways and the Payment Card Industry Data Security Standards in today's electronic marketplace. Next, a quantitative survey was administered to college-level students to validate the need to expand the course curriculum. Lastly, suggestions for future studies are provided to help bridge the gap between academia and the corporate world. When combined, this information will equip students with the needed knowledge to succeed when they enter the e-commerce workforce.

Keywords: Payment Gateways, Data Security Standards, Electronic Payment Systems
DOI: 10.7176/JEP/12-3-21
Publication date: January 31st 2021

1. Introduction

E-commerce has become a mainstay in the way consumers obtain services and products. The Internet has opened doors for businesses to expand their reach across the globe. Devices such as laptops, smartphones, and tablets have become today's storefronts. Online payment options have made cash payment systems virtually obsolete. More importantly, social media's proliferation has acted as a guiding agent for purchasing decisions; mobile e-commerce has evolved into one of the most significant driving forces into how businesses generate revenue [1]. This project aims to conduct a study centered on payment gateways (PGs) and Payment Card Industry Data Security Standards (PCI-DSS). The primary intent is to collect information that would enhance an undergraduate e-commerce course.

2. Background

E-commerce, as defined by Laudon and Traver [2], is "the use of the Internet, the Web, and mobile apps and browsers running on mobile devices to transact business" (p. 9). The transactional relationship between buyer and seller determines the e-commerce classification. The three primary models include Business to Consumer (B2C), Business to Business (B2B), and Consumer to Consumer (C2C). Subsets of these models include Mobile E-commerce (M-commerce), Social E-commerce, and Local E-commerce. An additional and more recent model, classified as Consumer to Business (C2B), entered the e-commerce arena when customers began to recommend products and services to companies [3] Inextricably linked to the Internet, e-commerce falls into three periods of development: invention, consolidation, and reinvention [2] During the invention period, from 1995-2000, the focus was on experimentation and earning brand recognition as a first-mover advantage in the retail marketplace. The next period, between 2001 and 2006, known as consolidation, generated a shift of focus from a technology-driven approach to a business-driven approach. Due to the rise of personal computers (PCs) in the home and the Internet, businesses began to expand their products to include services. The current period which began in 2007, is classified as the reinvention period. With the introduction of iPhones, mobile apps, and cloud computing, many e-commerce companies have started to use social, mobile, and local platforms.

2.1 E-Commerce Trajectory

Predictions for the continued growth of e-commerce are easily validated with a simple Internet search. For example, the U.S. Census Bureau [4] reported that retail e-commerce sales for the third quarter of 2019 in the U.S. reached 154.7 billion, which was a 5.0 percent increase from the second quarter of the same year. The data confirmed that e-commerce sales accounted for 10.5 to 11.2 percent of the total U.S. sales. These findings were derived from data obtained from Monthly Retail Trade Surveys (MTRS) and analyzed with a 90% confidence level.

Coexisting with the steady rise of e-commerce is the increased need for skilled and knowledgeable workers in the industry. Torpey [5] shared a report posted on the Bureau of Labor and Statistics' website, which revealed that employment in e-commerce industries increased by 80% from 1997 to 2016. The expectation is that the number of industry jobs will reach approximately 450,000 by 2026.

Viewed as a negative, the rise of e-commerce has also led to an upsurge of security and privacy breaches. Wertz (2019) shared a publicized report, sourced from Statista, stating that data breaches in the U.S. rose from 36.6 million in 2016 to 197.6 million in 2017. In 2018, the number of breaches reached a record high of 446.5 million. These numbers are likely to continue to escalate. Therefore, today's students must comprehend payment gateways and security measures to ensure that all parties involved are protected when utilizing an electronic payment system

3. Background Studies

A quantitative study by Nilashi et al. [7] focused on the critical need to build trust in developing B2C e-commerce websites. The purpose of their study was to evaluate the relationship (the level of intensity) that users place on security, familiarity, and design of e-commerce websites. The researchers developed two surveys using a 5-point Likert-scale. Ten experts in the e-commerce field responded to the first survey. A second survey, sent after analyzing the first survey, was completed by 150 e-commerce customers and IT students. An analysis of the collected data revealed that the design and familiarity of a site as a high priority. However, security was overwhelmingly ranked as the most important, thereby earning the highest intensity from all parties concerned.

Vakeel et al. [8] performed a comparative analysis of various B2B and B2C security and privacy requirements with a focus on vendor perspectives. For their study, the researchers collected data from 200 e-commerce sites to understand the difference in perceptions of vendors associated with each of the distinct models. After applying a regression analysis to the collected data, the results proved that vendors from both groups considered privacy equally important. However, security perceptions were viewed differently by B2B vendors. These results indicated B2B vendors' focused more on the security of data, processes, and legal aspects of the website. In contrast, B2C vendors focused their efforts on intimacy and restriction aspects of privacy on their websites. Many consumers reported a willingness to compromise privacy in exchange for the ability to shop online at their convenience.

A research analysis written by Kohli [9] provided consumers and organization leaders with an overview of technology terms and safeguards centered on security issues that commonly occur with the use of B2C and C2C e-commerce transactions. The implementation of authentication, authorization, encryption, auditing, integrity, nonrepudiation, and feature availability aids in the building of secure systems, yet they do not guarantee the site will be safe from cyber-attacks. Whether conducted over the intranet, extranet, or the Internet, all transactions are subject to fall prey to malicious attacks. Malware comes in various forms such as viruses, worms, Trojan horses and bots, unwanted programs that can change browser settings, and even spyware or adware that can lead to the collection of personal data and identity theft. Known technology approaches used to safeguard against such attacks are encryption, secure socket layer (SSL) protocols, secure hypertext transfer protocols (HTTPS), digital signatures, and digital certifications. A secure website, per Kohli (2016), requires the integration of a cyber-risk management team, collaborative relationships between partners, and an understanding that "there is not enough talent to do everything in-house; thus, a strategic approach to sourcing decisions is warranted" (p. 3). In other words, the author supports informed decisions are a necessary component when developing e-commerce websites.

Online Consumer Fears (OCF) was the focus of an empirical quantitative study conducted by researchers El Haddad et al. (2018). The purpose of their research was to find answers to the following three questions: (a) what factors drive customer payment decisions, (b) does a level of trust help customers overcome online fears, and (c) do financial fears impact privacy concerns? A total of 392 participants, with an online shopping experience of at least twice a month, responded to a 57 question survey about their online purchasing behavior. The results reinforced the hypothesis that a positive perception of quality, ease of use, and indicators of a secure website, play an essential role in the customer's decision to make an online purchase. The data further supported, although moderately, the fact that negative perceptions of the same factors lead to financial fears and lack of trust when making online payments. For this reason, the authors maintain that additional research is needed to develop more strategies to help reduce transaction fears.

4. Research Questions

As outlined above, the related works provided validation that students who plan to enter the e-commerce workforce following graduation need advanced PGS and PCI-DSS knowledge. Thus, the two researched questions that evolved from this study are as follows:

1. After completing an e-commerce college-level course, would students be able to define or describe PGs?
2. After completing an e-commerce college-level course, would students be able to define or describe PCI-DSS?

5. Methodology

The methodology deployed to answer the research questions was quantitative in nature. The target was an e-commerce class that had 24 students enrolled in spring 2020. A 21-question survey was conducted, and the survey was divided into three sections. The first section asked students to read and sign an IRB approved Informed Consent Form, confirm their status as a sophomore or senior, and state their majors/minors. The second section asked specific knowledge related questions about PGs and PCI-DSS. Several of the questions were open-end which allowed students to offer their vision as to the importance of learning the material. The last section consisted of two questions, which asked students to share their vision on how this material should be taught to be conducive to their learning style.

The answers to the questions are then used in the analysis to determine how much about PGs and PCI-DSS knowledge they already possessed and how much more they need to learn.

6. Data Analysis

The survey was administered during the last week of an e-commerce class during the spring 2020 semester. Completion was voluntary and not associated with a grade. 18 out of the 24 students in the class responded. The sophomore to senior ratio was 2-to-16. Their majors/minors were equally divided between IT Security, Digital Media, Software Devolvement, Enterprise Systems, and Management Information Systems.

Of interest, is the fact that the number of no responses to the questions "If asked during a job interview would you be able to define or describe PGs or PCI-DSS?" were 44.4% and 72.2% respectively. See Tables1 below. When asked to define the terms, one student wrote, "Payment processing software used to let people purchase/pay for goods online." This is important to note, as a payment gateway is not the same as payment processing software.

	Yes	No
Payment Gateways	10 (55.5%)	8 (44.4%)
PCI-DSS	5 (27.7%)	13 (72.2%)

Table 27: Students' knowledge level of PGs and PCI-DSS.

Further validation of the need to enhance the core e-commerce knowledge is implied by the students' lack of knowledge about PCI-DSS requirements. When asked how original requirements were preserved in the 2018 revision, only 33.3% percent knew the answer was 12. See table 2 below. Due to the set options and based on equally distributed selections, it is likely that the correct answers could have been guesses vs. actual knowledge.

Requirements	Frequency	Percent
10	5	55.5%
12	6	33.3%
15	6	23.3%
20	1	5.6%
Total	18	

Table 28: Students' knowledge of PCI-DSS requirements

Finally, when the students were asked if they believed that PGs and PCI-DSS should be enhanced in the current core curriculum, the yes to no responses were 14 to 4, respectively.

7. What is Electronic Payment Systems

While there is an abundance of studies focused on e-commerce concerns and challenges, a limited few provide detailed information about the intricacies associated with understanding electronic payment systems. Therefore, this section defines Payment Gateways (PGs) and Payment Card Industry Data Security Standards (PCI-DSS). The section concludes with a high-level overview of five top payment gateway vendors.

7.1 Payment Gateways

Every transaction must pass through an electronic payment system, whether selling a product or service, selling to a business or consumer, or manufacturing and shipping by a third party [10]. More than 60 percent of all online purchases a credit or debit card [11]. While it may seem counter-intuitive, sales of this type classify as card-not-present transactions. Since the merchant cannot physically view the card, acceptance creates a degree of risk to all parties involved. A fraudulent transaction can adversely affect merchants, suppliers, banks, and consumers.

All online payment transactions involve two primary components: the payment acceptance process and the transaction clearing process [12]. The acceptance process performs functions to validate the card and its associated credit limit. Once validated, the transaction clearing process ensures the movement of funds from the cardholder to the merchant. These processes are accomplished through either a closed (unitary) or an open (distributed) loop system. In a closed-loop system, credit card issuers such as Discover and American Express interact directly with merchants and consumers; no other institutions are involved. In contrast, in an open loop-system, merchant banks issue cards to consumers on behalf of credit card associations such as Visa and MasterCard. The introduction of a third party creates a more involved payment process but still uses the same principles.

Included in the mix of electronic payment transactions are those that involve the use of mobile devices. The processing of mobile payments (m-payments) is accomplished in one of two ways: via a remote payment system or a proximity payment system [13][26]. The remote system requires devices to be connected to cellular radio or Wi-Fi networks. In contrast, the proximity system requires connections to contactless technologies such as near field communication (NFC) or quick response (QR) codes to complete a transaction. The proximity payment process is similar to the steps for the credit card process. The customer swipes the mobile device close to the point of sale (POS) to initiate the transaction. Data is sent via a gateway to a payment processor and validated for fraud. Next, the transaction is sent to the issuer for authorization of payment. After receiving assurance that funds are available, the merchant fills the order. The payment is transferred from the issuer to the merchant’s account.

Although the general processes may appear simple, designing a payment system is a complicated task. Large firms typically hire skilled workers to implement and maintain an in-house system, whereas medium and small companies rely on payment gateways (PGs) to process their transactions [14]. PGs are service provided applications that offer authorization of online credit card transactions. “They authenticate and route payment details in an extremely secure environment between various parties and related banks" [15]. In simpler terms, the gateway takes on the role of an intermediary between the merchant and the consumer. They perform the magic behind the screen, validate the input data matches the card, which helps protect the consumer’s personal and private information. [16]

7.1.1 Benefits and Features

Payment Gateways do not come in a one-size-fits-all platform. Benefits and features vary from vendor to vendor, which makes the choice of selecting just the right one for a specific business a daunting task [17]. To offer guidance with the selection process, Alton suggested merchants compare features such as compatibility, reporting and invoicing options, speed and user experience, and cost to determine the best fit for their business. Adding to this list, Alton stressed the importance of evaluating the PG's fraud detection methodologies, security features, and encryption standards to protect both the business and the consumer.

Encryption dates back to the ancient Egyptian and Greek times when the sender and the receiver [2] encrypted secret messages into a code that could only be read by those with the secret codes. The encryption process requires developing a mathematical algorithm, referred to as a key, comprised of a string of 128, 256, or 512 binary digits. In a face-to-face environment, the message and the key are delivered directly to the receiver; thus, the transaction is secure. In the online environment, messages and keys are delivered via an open, unsecured, and shared transmission media such as cables or Wi-Fi. Packets sent through this method are vulnerable to interception and data breaches. Over 8,500 data breaches and over 11 billion consumer records have been compromised, according to a Privacy Rights Clearinghouse report cited. [18]

Encryption techniques, like the Internet, have improved over time. Today's symmetric and asymmetric cryptography techniques can offer message integrity, nonrepudiation, identity authentication, and confidentiality to e-commerce users [2]. Symmetric cryptography works with one key shared by both the sender and receiver called a private key. Asymmetric cryptography works with two keys: a private key and a widely disseminated public key. The selection of an appropriate key for a specific application can be a challenge due to differences such as latency, key size, and security concerns. [27] Nevertheless, the use of cryptography is the best way to maintain a secure online platform.

7.2 Payment Card Industry Data Security Standards (PCI-DSS)

In 2004, American Express, Discover, JCB, MasterCard, and Visa banded together to establish Payment Card Industry Data Security Standards (PCI-DSS). The purpose of their initiative was to replace individual efforts with standard protocols to protect the storage and processing of sensitive credit card data [19]. The capture of authentication data such as magnetic strip information, primary account numbers (PAN), and credit card verification (CVV) can easily be used to impersonate cardholders and steal identities. The capture process is not limited to the cyber world; insiders have used physical and procedural controls to steal data [20]. To address all security concerns, the PCI Security Standards Council (PCI_SSC) developed standards to address technical, operational, and physical components attached to the payment transaction process.

The latest version of PCI-DSS, v3.2.1, released in May of 2018, preserved the 12 requirements developed in the original 2004 document. These requirements, several of which reinforce General Data Protection Regulations (GDPR) and Health Insurance Portability and Accountability Act (HIPPA) privacy laws, are organized under six logically related categories as follows: [20] [28] [21]

Build and Maintain a Secure Network
Protect Cardholder Data
Maintain a Vulnerability Management Program
Implement Strong Access Control Measures
Regularly Monitor and Test Networks,
Maintain an Information Security Policy

The first two requirements mandate installing a firewall and removing default passwords on all computers and systems that capture cardholder data. The next two requirements provide encryption criteria for the storage and transmissions of card sensitive data.[20] emphasized the importance of restricting storage to essential data only and using wired *vs.* wireless transmission when possible. Standards for requirements 5 and 6, focus on the application of security systems, such as the installation and maintenance of anti-virus software. Next, requirements 7, 8, and 9 focus on implementing access controls to physical computers and authentication of authorized personnel. Data is required to be backup offsite in an encrypted format. Processes to monitor, test, and audit networks and security systems are described in requirements 10 and 11. Lastly, requirement 12 states that information security policies must be disseminated to all employees in clear, simple, and understandable terms. [20] [19]

Every business that accepts, processes, or stores credit card data is required to be PCI-DSS compliant in one of four levels (Dahn, 2019).[28] The levels are contingent upon the volume of transactions processed on an annual basis. Organizations with annual transactions of over six million are placed in the Level 1 category. Level 1 is the highest category with the most stringent requirements. Level 2 is reserved for organizations with annual transactions between one to six million. Level 3 is reserved for annual transactions between 20,000 and one million.

Startups and small businesses, those with fewer than 20,000 annual transactions, fall into the Level 4 category. Regardless of size, every organization must complete an appropriate annual assessment report, perform a quarterly network scan by an Approved Scan Vendor (ASV), and provide an Attestation of Compliance (AOC) for Onsite Assessment to maintain compliance accreditation. The specifications for each category is beyond the scope of this paper. However, to offer an overview of payment systems and criteria, the next section highlights five popular PCI-DSS Level 1 compliant Payment Gateways.

7.3 PG Vendors

The following is not an all-inclusive list of Level 1 PG vendors, nor is it in support of any specific vendor. Instead, this section provides a brief overview of each vendor for students' use in future comparative analysis. The summaries, listed in alphabetical order, highlight features such as compatibility, reporting and invoice options, user experience, fraud detection, security features, encryption standards (when available), and cost.

7.3.1 2checkout

2checkout, formally Avangate was officially launched in 2006 as an e-commerce solution provider to help vendors increase their revenue through online channels. Today, the company is recognized internationally, has over 17,000 active clients, and operates out of four global offices (Hart, 2020). Their payment processor integrates with over 100 shopping carts, including popular e-commerce platforms such as Shopify and Bigcommerce. Implementation is made simple with payment Application Program Interfaces (APIs) written in languages such as PHP, Python, and Java. Developer tools and easy to navigate dashboards allow for customization. For security measures, 2checkout employs advanced fraud protection, a three-tier defense strategy for real-time detection. It adheres to all Level 1 PCI compliant requirements. Their customer support includes an online FAQ knowledge and policy page, available for general questions, contact information for calls or email, and a strong presence on social media. The cost of their product is dependent upon the service selected. The 2SellPlan, for those selling internationally, is 3.5% plus $0.35 per sale. For the 2SubsribePlan, for selling subscriptions, the rate is 4.5% plus $0.45 per sale. Finally, for the 2MonetizePlan, for digital items, the rate is 6% plus $0.60 per sale [21]

7.3.2 Authorize.Net

Authorize.net, founded in 1996, is one of the older payment gateway service providers on the web (Karol, 2020).[22] Leading e-commerce platforms such as Shopify, Volusion, and BigCommerce offers customers the ability to integrate Authorize.Net as the PG for their online stores (Zorzini, 2018).[23] Finance management analysis is easily accomplished due to data import options available with the syncing of QuickBooks and the company's Transaction Details API. Advanced fraud detection and security protection features include customizable rule-based filters, tokenization of sensitive customer information, assistance with installation and maintenance of firewalls, and adherence to all 12 requirements mandated by PCI to maintain Level 1 compliance. Customer support is offered support 24/7, except for holidays. The company offers two pricing systems: (1) an all-in-one option for businesses without a merchant account and (2) a payment gateway only option for business with a merchant account. The cost for the first is $25 per month and 2.9% plus $0.30 for each transaction. The cost for the second is also $25 per month plus $0.10 for each transaction [22] [23]

7.3.3 Payline

Payline, launched in 2009 and headquartered in Chicago, offers flexible and friendly payment processing solutions for businesses regardless of size and industry (paylinedata.com/about/). Companies equipped with Payline's developer documentation and APIs have the freedom to design a system specific to their individual needs. Financial reports and invoices are made easy to integrate with financial and accounting software such as QuickBooks [24]. Access to third-party security programs like Ethoca and Verify provides high-level fraud protection. Customer support is available during regular business hours Monday to Friday. Pricing calculations are derived from the interchange-plus model; it applies the specific card's processing fee to 0.3% of the transaction amount. On the positive side, the company offers month-to-month contracts with no early termination fees for the cancelation of services. Payline also believes in Corporate Social Responsibility (CSR); they give a portion of their profits to charity each month and offer discounts to businesses with registered charities.

7.3.4 PayPal

PayPal is the most recognized online payment processing system used in personal and business environments. However, for this section, the summary focuses on the PayPal Commerce Platform and its design as an e-commerce solution provider. Plans and services offered include PayPal Express Checkout, PayPal Payment Standard, and PayPal Payment Pro. The difference between the three is the checkout process. The Payment Pro option allows customers to remain on the e-commerce site for the entire purchase *vs.* being redirected to PayPal to authorize payment. [22][23] Regardless of choice, PayPal experts offer help to simplify and manage Payment Service Directives (PSD2), PCI-DSS, and Office of Foreign Assets Control (OFAC) sanctions and global compliance mandates. Real-time intelligence and adaptive machine learning provide fraud protection and security measures. Their live global support team recommends solutions to implement and optimize the integration of their systems onto the customer's e-commerce site (www.paypal.com/us/webapps/mpp/commerce-platform). The cost associated with each option is 2.9% plus $0.30 per transaction, with an additional $30 per month for the Payment Pro option. [22]

7.3.5 Stripe

Stripe, launched in 2011, is an American based technology company that offers a complete payment system for online and in-person payments (Stripe.com, 2020). Stripe is offered in over 26 countries, mostly in Europe and the Americas, with a beta version in India. Their processing system is customizable and scalable with an application-programming interface (API); therefore, it integrates well into online stores. Billing tools assist with creating and managing subscriptions, mobile app purchases, price testing, and sending out invoices. Instances of fraud are reduced by up to 25% with machine learning, a dashboard for setting purchasing rules, and the implementation of two-factor authentication [22]. Transaction security is further guaranteed with the use of Advanced Encryption Standards (ASE-256) encryption keys. The company offers support 24/7 at the cost of 2.9% plus $0.30 per credit card transaction in the United States, and an additional 1% for the use of international cards. [16]

8. Conclusion and Future Research

The literature review, the electronic payment discussions, the synopsis of the five PG vendors, and the results from the quantitative survey all provide evidence that students need enhanced knowledge of PGs and PCI-DSS before entering the workforce. Chen et al. [29] reminded readers that E-commerce and the acceptance of electronic payments had become a competitive necessity for businesses operating in today's global market. Even Walmart, the Goliath in the brick-and-mortar retail industry, has taken great strides to change their brand to that of an omni-channel retailer [2].

Payment gateways (PGs) function as an intermediary between merchants and consumers to authorize online credit card transactions; however, they do not offer a universal solution that best fits every company. The selection of a PG for a specific company can be a challenge due to the variety of individual vendors' features and benefits. In contrast, businesses are assigned a PCI-DSS level based on the volume of transactions they process annually. Regardless of level, every company that accepts electronic payments must adhere to the 12 standardized requirements designed to protect the storage and processing of sensitive credit card data.

A review of the analysis shows that PGs and PCI-DSS are topics that need to be added to the e-commerce course objectives to prepare students for real-world e-commerce industry skills. Further research can be done on how effective these new learning topics after several semesters of teaching the updated content.

References

[1] Kyle Wong. 2018. Top 5 trends driving e-commerce: influential takeways from the report retailers cannot ignore. *Forbes*. Retrieved from https://www.forbes.com/sites/kylewong/2018/06/07/top-5-e-commerce-takeaways-from-the-most-influential-report-of-the-year/#3001579c5696

[2] Kenneth C. Laudon and Carol G. Traver. 2020. *E-Commerce busines. technology. society* (15th edition*).* Pearson.

[3] Chandrasegar Thirumalai and Murugesan Senthilkumar. 2017. An assessment framework of intuitionistic fuzzy network for C2B decision making. *In 2017 4th International Conference on Electronics and Communication Systems (ICECS) (pp. 164-167).* IEEE. doi: 10.1109/ECS.2017.8067861

[4] U.S. Census Bureau, 2019. Quarterly retail e-commerce sales 1st quarter 2019. Retrieved from https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf

[5] Elka Torpey. 2018. Employment growth and wages in e-commerce. *U.S. Bureau of Labor Statistics*. Retrieved from https://www.bls.gov/careeroutlook/2018

[6] Jia Wertz. 2019. While data breaches accelerate, it's critical that e-commerce businesses stay safe. *ForbesWomen*. Retrieved from https://www.forbes.com/sites/jiawertz/2019/09/19/while-data-breaches-accelerate-its-critical-that-e-commerce-businesses-stay-safe/#2a5149bd4f5c

[7] Mehrbakhsh Nilashi, Karamollah Bagherifard, Othman Ibrahim, Nasim Janahmadi, and Mousa Barisami. 2011. An application expert system for evaluating effective factors on trust in B2C websites. *Engineering, 3*(11), 1063-1071. doi:10.4236/eng.2011.311132

[8] Khadija A. Vakeel, Saini Das, Godwin J. Udo, and Kallol Bagchi. 2017. Do security and privacy policies in B2B and B2C e-commerce differ? A comparative study using content analysis. *Behaviour & Information Technology, 36(4),* 390-403. doi: 10.1080/0144929X.2016.1236837

[9] Gautam Kohli. 2016. E-Commerce: Transaction security issue and challenges. *CLEAR International Journal of Research in Commerce & Management, 7*(2).

[10] Rashidah F. Olanrewaju, Burhan U. I. Khan, Mohd. Mueen U. I. Matto, Farhat Anwar, Anis N. B. Nordin, and Roochie N. Mir. 2017. Securing electronic transactions via payment gateways a systematic review. *International Journal of Internet Technology and Secured Transactions, 7(*3), 245-69. doi: 10.1080/0144929X.2016.1236837

[11] Gary P. Schneider. 2017. *Electronic Commerce* (12th edition). Cengage Learning.

[12] Lorrie Willey and Barbara J. White. 2013. Do you take credit cards? Security and compliance for the credit card payment industry. *Journal of Information Systems Education, 24*(3), 3.

[13] Ming-Hsiung Hsiao. 2019. Mobile payment services as a facilitator of value co-creation: A conceptual framework. *The Journal of High Technology Management Research, 30*(2), 100353. doi: https://doi.org/10.1016/j.hitech.2019.100353

[14] Ghada El Haddad, Esma Aïmeur, and Hicham Hage. 2018. Understanding trust, privacy and financial fears in online payment*. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 28-36). IEEE. doi: 10.1109/TrustCom/BigDataSE.2018.00015

[15] Ved P. Gulati and Shilpa Srivastava. 2007. The empowered internet payment gateway. *In International Conference on E-Governance* (pp. 98-107).

[16] Karol K. 2020. What is a payment gateway? Plust 5 of the best payment gateways copared for 2019. *Ecommerce Platforms.* Retrieved from https://ecommerce-platforms.com/ecommerce-selling-advice/choose-payment-gateway-ecommerce-store

[17] Larry Alton. 2017. 9 things to look for in a payment gateway. *Entrepreneur.* Retrieved from https://www.entrepreneur.com/article/294964

[18] Mike Dahn. n.d.. A guide to PCI compliance. *Stripe.* Retrieved from https://stripe.com/guides/pci-compliance

[19 Alex Hart. 2020. About 2Checkout. Retrieved from https://www.2checkout.com/about/

[20] Clive Blackwell. 2008. The management of online credit card data using the Payment Card Industry Data Security Standard. *In 2008 Third International Conference on Digital Information Management (pp. 838-843).* IEEE. doi: https://doi.org/10.1109/icdim.2008.4746843

[21] PCI Security Standards Council, 2020. Maintaining Payment Security. Retrieved from https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

[22] Joe Warnimont. 2020. A detailed 2checkout review (February 2020): one of the best payment gateways. *Ecommerce Platforms.* Retrieved from https://ecommerce-platforms.com/ecommerce-reviews/2checkout-review-payment-gateway

[23] Catalin Zorzini. 2018. Authorize.net reveiws & fees for merchant account. *Ecommerce Platforms.* Retrieved from https://ecommerce-platforms.com/ecommerce-reviews/authorize-net-review-payment-gateway

[24] Catalin Zorzini. 2020. In-depth paypal reviews (February 2020): Is paypal the right payment platform for you? *Ecommerce Platforms.* Retrieved from https://ecommerce-platforms.com/ecommerce-reviews/paypal-reviews

[25] Joe Warnimont. 2019. Stripe review: payment processor with advanced development and clear pricing. *Ecommerce Platforms.* Retrieved from https://ecommerce-platforms.com/ecommerce-reviews/stripe-review

[26] Amy J. C. Trappey, Charles V. Trappey, and Abby P.T. Hsu. 2016. Patent portfolio analysis of e-payment services using technical ontology roadmaps. *In 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 004824-004829).* IEEE. doi: 10.1109/SMC.2016.7844992

[27] MNB Anwar, M Hasan, MM Hasan, JZ Loren, and S.M.T Hossain. 2019. Comparative Study of Cryptography Algorithms and Its' Applications. *International Journal of Computer Networks and Communications Security, 7*(5), 96-103.

[28] Ecommerce Platforms Editorial Team, 2019. Payline data reviews: a transparent payment gateway with online, in-store and mobile solutions. *Ecommerce Platforms.* Retrieved from https://ecommerce-platforms.com/ecommerce-reviews/payline-data-review-a-merchant-account-provider-with-a-conscience

[29] Alexander N. Chen, Steven M. Zeltmann, Ken Griffin, Michael Rubach, & Michael E. Ellis. 2019. Trends and Technology in E-Payment. *In Competition Forum* (Vol. 17, No. 2, pp. 402-412). American Society for Competitiveness.

[30] Stripe.com, n.d.. Our mission is to increase the GDP of the Internet. *Stripe.* Retrieved from https://stripe.com/about

[31] Paylinedata.com, 2020. Experience payments differently. Retrieved from https://paylinedata.com/about/

[32] PayPal.com, 2020. Say hello to the PayPal commerce platform. PayPal. Retrieved from https://www.paypal.com/us/webapps/mpp/commerce-platform