GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(REVIEW ARTICLE)

Check for updates

Securing the virtual marketplace: Navigating the landscape of security and privacy challenges in E-Commerce

George Caleb Oguta *

Jaramogi Oginga Odinga University of Science & Technology, Kenya.

GSC Advanced Research and Reviews, 2024, 18(01), 084–117

Publication history: Received on 15 November 2023; revised on 06 January 2024; accepted on 09 January 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.18.1.0488

Abstract

This paper provides a comprehensive examination of the evolving challenges and critical considerations surrounding security and privacy within the realm of e-commerce. As the digital marketplace continues to expand, the significance of safeguarding sensitive information and ensuring user privacy has become paramount. This paper explores various dimensions of security threats, including data breaches, phishing attacks, and vulnerabilities associated with payment gateways, shedding light on the potential repercussions for businesses and consumers alike. Additionally, it delves into emerging technologies and innovative solutions aimed at fortifying e-commerce platforms against evolving cyber threats. The paper not only identifies the existing vulnerabilities but also proposes proactive strategies and future directions for research and implementation. Topics such as biometric authentication, post-quantum cryptography, and privacy-preserving technologies are explored as potential avenues for enhancing the security posture of e-commerce systems. The research presented emphasizes the critical intersection of technology, regulation, and user awareness in fostering a secure and trustworthy online shopping environment. By offering insights into both the current state of e-commerce security and promising avenues for future exploration, this paper aims to contribute to the ongoing discourse on fortifying the digital marketplace against the challenges posed by an ever-evolving cyber landscape.

Keywords: E-commerce; Attacks; Privacy; Security; Performance; Cyber threats; Data breaches; User authentication

1. Introduction

E-commerce, or electronic commerce, represents the digitalization of traditional commerce, enabling the buying and selling of goods and services over the internet [1]. This revolutionary concept has evolved significantly since its inception, reshaping the global business landscape. One of the key aspects of e-commerce is the establishment of online retail platforms, where businesses can showcase and sell their products to a vast audience. This shift has transcended geographical boundaries, allowing consumers to access a diverse array of products from anywhere in the world. According to [2], E-commerce, a cornerstone of the digital age, has revolutionized the way businesses operate and consumers engage in commerce. At its core, electronic commerce involves the buying and selling of goods and services facilitated through the internet. This dynamic shift from traditional brick-and-mortar transactions to online platforms has fundamentally transformed global trade and consumer behavior [3]. As shown in Figure 1, E-commerce encompasses a diverse range of activities, from retail giants like Amazon offering a myriad of products to small businesses leveraging digital storefronts to reach a broader audience.

The fundamental appeal of e-commerce lies in its unparalleled convenience. Consumers can browse, select, and purchase products from the comfort of their homes, breaking free from the constraints of physical store locations and operating hours [4]. This accessibility has democratized commerce, allowing businesses of all sizes to compete on a global scale. Moreover, the rise of mobile commerce (m-commerce) has further accelerated this trend, as smartphones enable users to shop on the go, blurring the lines between online and offline experiences.

* Corresponding author: George Caleb Oguta

The advent of e-commerce has not only changed how businesses operate but has also transformed consumer behavior. With the convenience of online shopping, consumers can browse, compare, and make purchases at any time, breaking away from the constraints of traditional brick-and-mortar store hours [5], [6]. This convenience factor, coupled with the ability to access a wide range of products and services, has contributed to the rapid growth and widespread adoption of e-commerce across various industries. Security is a critical consideration in e-commerce due to the sensitive nature [7] of online transactions. Businesses invest in technologies such as secure socket layer (SSL) encryption and two-factor authentication to safeguard customer data and build trust. Moreover, the integration of data analytics plays a pivotal role in e-commerce operations. By analyzing customer behavior and preferences, businesses can tailor their offerings, enhance user experiences, and optimize pricing strategies.

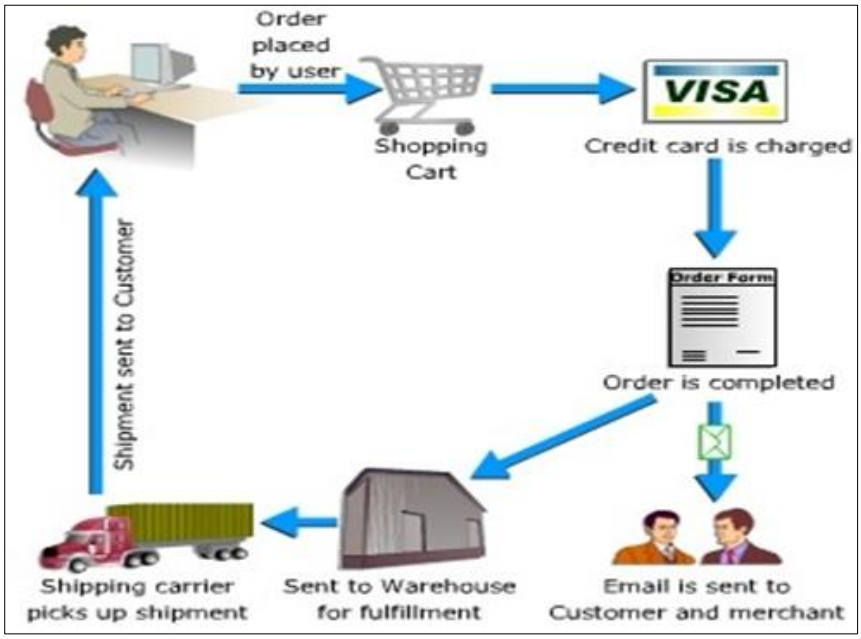

Figure 1 E-commerce operation

According to [8], security is a paramount concern in e-commerce due to the sensitive nature of online transactions. Establishing and maintaining trust between businesses and consumers requires robust cyber-security measures. Technologies such as encryption protocols and secure payment gateways are critical in safeguarding personal and financial information [9]-[12]. Additionally, the collection and analysis of vast amounts of data through advanced analytics play a pivotal role in tailoring marketing strategies, enhancing user experiences, and optimizing supply chain management.

Despite its numerous advantages, e-commerce faces challenges such as cyber-security threats, logistical complexities, and regulatory compliance [13]. Ensuring a seamless supply chain and addressing these challenges are essential for the sustained success of e-commerce businesses. As technology continues to advance, innovations like mobile commerce, social commerce, and emerging technologies such as artificial intelligence promise to further shape the future of e-commerce, providing new opportunities and challenges for businesses and consumers alike. In addition, e-commerce faces challenges that range from logistical intricacies to regulatory compliance [14]. Efficient supply chain management, including inventory control and timely order fulfillment, is crucial for meeting customer expectations. Regulatory frameworks related to online transactions, data privacy, and consumer protection add layers of complexity that businesses must navigate. As technology continues to advance, the future of e-commerce holds exciting possibilities, with innovations like augmented reality and artificial intelligence promising to reshape the online shopping experience. In essence, e-commerce stands as a transformative force, shaping the present and future of commerce on a global scale.

2. E-commerce architecture

E-commerce architecture refers to the structure and components of the systems and infrastructure that enable electronic commerce operations [15]. The architecture of an e-commerce platform is designed to support various functionalities, including product catalog management, order processing, payment transactions, and user interactions. Figure 2 presents an overview of the e-commerce architecture.

The following is an overview of the key components and layers commonly found in e-commerce architecture:

2.1. User Interface Layer

The User Interface (UI) Layer in e-commerce refers to the front-end components and elements that users interact with when navigating an online platform [16]. It is the visual and interactive part of the e-commerce system that allows users to browse products, make selections, and complete transactions. The primary goal of the UI Layer is to provide a user-friendly and visually appealing experience, encouraging visitors to explore the website or application and ultimately make purchases. Key aspects of the User Interface Layer in e-commerce include:

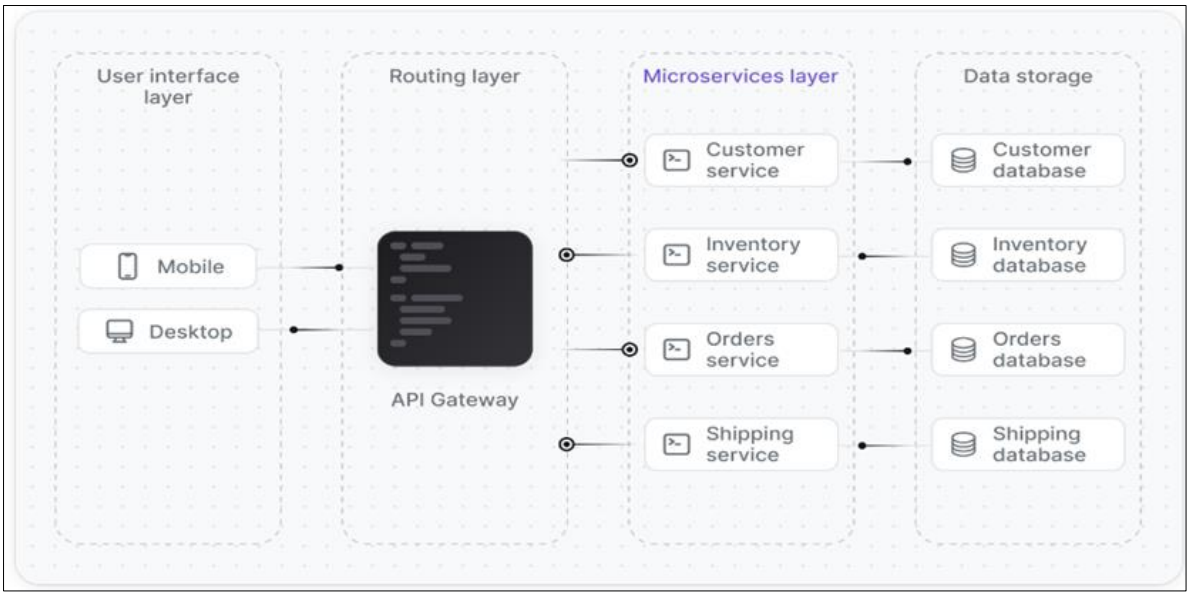

Figure 2 Overview of the e-commerce architecture

2.1.1. Website Design and Layout

Website design and layout in e-commerce play a pivotal role in shaping the overall user experience and influencing customer engagement and conversion. A well-crafted design involves intuitive navigation menus that guide users effortlessly through product categories, featured promotions, and essential sections [17]. The homepage serves as a visually appealing entry point, showcasing key offerings and establishing the brand's identity. Product listings are organized in a visually compelling manner, featuring high-quality images, concise descriptions, and clear pricing. The design extends to detailed product pages that provide comprehensive information, user reviews, and a seamless path to add items to the shopping cart. Responsive design ensures a consistent and user-friendly experience across devices, enhancing accessibility. Effective e-commerce website design is not only aesthetically pleasing but also strategically influences user behavior, facilitating a smooth and enjoyable shopping journey that encourages visitors to explore, engage, and complete transactions. Particularly, the following are critical:

Navigation Menus: Intuitive navigation menus help users easily find product categories, search for specific items, and explore different sections of the online store.

Homepage: The homepage typically showcases featured products, promotions, and important announcements. It serves as the gateway to the rest of the e-commerce site.

2.1.2. Product Presentation

Product presentation in e-commerce is a critical element that directly influences customer engagement and purchase decisions. It involves the strategic display of products with the aim of providing users with a visually appealing and informative experience [18]. Well-designed product listings showcase essential details such as high-quality images, prices, and concise descriptions, allowing users to quickly evaluate and compare items. Detailed product pages further enhance the presentation by offering in-depth information, specifications, customer reviews, and additional images. This comprehensive presentation not only facilitates informed decision-making but also contributes to a positive perception of the brand. The goal is to create a compelling and user-friendly environment that encourages users to

explore products, ultimately leading to increased trust and higher conversion rates. Product listings and pages are especially important in this perspective.

- *Product Listings*: Well-designed product listings display essential information such as product images, prices, and brief descriptions. Users can quickly scan through products and click on items of interest.
- *Product Pages*: Detailed product pages provide in-depth information, specifications, customer reviews, and additional images. Users can make informed decisions before adding items to their cart.

2.1.3. Shopping Cart and Checkout

The shopping cart and checkout process in e-commerce are pivotal stages where user experience can significantly impact the conversion rate. The shopping cart serves as a virtual repository for selected items, allowing users to review and modify their choices before proceeding to checkout. A user-friendly cart interface displays itemized details, including quantities and prices, while offering transparency on additional costs like shipping [19]. The checkout process, often comprising multiple steps, guides users through entering shipping information, selecting payment methods, and confirming their orders. An optimized and intuitive shopping cart and checkout design minimizes friction, ensuring a seamless transition from product selection to finalizing the purchase. Clear calls-to-action, transparent pricing, and secure payment options contribute to a positive user experience, fostering trust and encouraging customers to complete their transactions. The following are particularly important in this respect.

- *Shopping Cart*: The UI for the shopping cart allows users to review the items they've selected, adjust quantities, and proceed to checkout. It may also display relevant information such as estimated shipping costs and taxes.
- *Checkout Process*: The UI for the checkout process guides users through steps such as entering shipping information, choosing payment methods, and reviewing their order before finalizing the purchase.

2.1.4. User Account and Personalization

User accounts and personalization are integral components of e-commerce, enhancing the overall customer experience and fostering brand loyalty. User accounts enable customers to create profiles, track order history, and manage preferences, providing a convenient and personalized interface for returning visitors. Through personalization, e-commerce platforms leverage user data to tailor recommendations, showcase relevant products, and create a more customized shopping journey [20]. Features like wishlists, favorites, and saved addresses contribute to a seamless and efficient shopping experience, making it easier for users to navigate, engage with, and ultimately make purchases on the platform. The combination of user accounts and personalization not only facilitates convenience but also plays a crucial role in building a long-term relationship between the customer and the e-commerce brand. *User accounts* as well as *wishlists and favorites* are described below.

- *User Accounts*: The UI allows users to create accounts, log in, and manage their profiles. Registered users often benefit from personalized experiences, including order history, saved preferences, and recommended products.
- *Wishlists and Favorites*: Users can save items for future reference, creating wishlists or marking products as favorites for easy access during subsequent visits.

2.1.5. Responsive Design

Responsive design in e-commerce is a crucial strategy to ensure a consistent and optimal user experience across various devices such as desktops, tablets, and smartphones. By adapting the layout, content, and functionality to different screen sizes and resolutions, responsive design enables users to access and interact with an e-commerce website seamlessly, regardless of the device they use [21]. This approach not only caters to the diverse preferences of consumers but also addresses the increasing trend of mobile commerce. A well-executed responsive design enhances accessibility, minimizes the need for separate mobile applications, and contributes to higher user satisfaction by delivering a visually cohesive and user-friendly interface irrespective of the device, ultimately influencing customer engagement and conversion rates positively. *Cross-device compatibility* as used in this perspective, is discussed in some detail as follows.

- *Cross-Device Compatibility*: The UI Layer is designed to be responsive, ensuring a consistent and user-friendly experience across various devices such as desktops, tablets, and smartphones. This adaptability is crucial for reaching users regardless of the device they use to access the platform.

2.1.6. Visual Elements

Visual elements in e-commerce play a pivotal role in capturing and retaining the attention of online shoppers. From compelling product images and videos to an aesthetically pleasing website design, these elements significantly impact the overall user experience. High-quality and professionally presented product visuals not only showcase the details of items but also instill confidence in potential buyers [22]. Clear and intuitive navigation, along with consistent branding elements such as logos and color schemes, contributes to a visually cohesive and recognizable online presence. Visual elements extend to the overall layout of the website, including homepage banners, product listings, and checkout pages, influencing the way customers perceive and interact with the online store. In essence, the strategic use of visual elements in e-commerce enhances engagement, fosters brand identity, and ultimately contributes to higher conversion rates by creating an appealing and user-friendly shopping environment. The following concepts are crucial in this respect.

- *Images and Multimedia*: High-quality product images and, in some cases, videos enhance the visual appeal of the platform and provide users with a better understanding of the products.
- *Branding Elements*: Consistent use of branding elements, including logos, color schemes, and typography, reinforces the brand identity and contributes to a cohesive user experience.

2.1.7. Interactive Features

Interactive features in e-commerce are essential elements that engage and guide users throughout their online shopping journey. These features, such as dynamic sliders, pop-ups, and hover effects, enhance user interactivity and create a more immersive and enjoyable experience [23]. An effective search functionality allows users to quickly find products, while interactive product configurators or virtual try-on options enable a more personalized exploration. Interactive elements contribute to a sense of dynamism, guiding users through the platform, providing instant feedback, and fostering a more engaging connection with products and services. Furthermore, features like real-time chat support or customer reviews add a layer of interactivity that helps users make informed decisions. In essence, these interactive features in e-commerce not only improve usability but also play a crucial role in capturing and retaining the attention of online shoppers, ultimately influencing their purchasing decisions positively.

- *Search Functionality*: An effective search feature enables users to find specific products quickly by entering keywords or using filters. *Search functionality* and *interactive elements* are of significance as used in this respect.
- *Interactive Elements*: Interactive features such as sliders, pop-ups, and hover effects can enhance engagement and guide users through the shopping process.

A well-designed User Interface Layer is crucial for attracting and retaining customers in the competitive e-commerce landscape. It focuses on creating a positive and seamless user experience, ultimately influencing user satisfaction and conversion rates. Additionally, a user-friendly UI contributes to brand perception and customer loyalty.

2.2. Application Layer

The application layer in e-commerce constitutes the core functionality and business logic that governs the entire operation of online platforms [24]. At this layer, the e-commerce system manages critical processes such as inventory management, order processing, and transaction handling [25]. The business logic encompasses rules and algorithms that dictate pricing strategies, promotions, and the overall functionality of the e-commerce platform. Additionally, the Content Management System (CMS) resides within the Application Layer, overseeing the organization and presentation of digital content, including product information, images, and promotional materials. This layer is the engine that powers the user-facing aspects, ensuring a seamless and efficient e-commerce experience for both customers and administrators. Through the Application Layer, businesses can adapt to market dynamics, implement personalized features, and continually optimize their operations to meet the evolving demands of the online marketplace. *Business Logic* as well as *Content Management System* are of essence in this domain.

- *Business Logic*: The application layer contains the business logic that governs the functionality of the e-commerce platform. This includes rules for pricing, promotions, order processing, and other core business processes.
- *Content Management System (CMS)*: CMS manages and organizes digital content, including product information, images, and promotional content, ensuring consistency and relevance across the platform.

2.3. Data Layer

The data layer in e-commerce is the foundation for storing, managing, and retrieving vast amounts of structured information critical to the functioning of online platforms. At its core, the database within this layer houses essential data such as product details, customer profiles, order histories, and inventory status [27]. Whether utilizing relational databases or NoSQL solutions, the Data Layer ensures the integrity and availability of information for various e-commerce processes. Additionally, this layer supports data warehousing and analytics, enabling businesses to derive valuable insights into customer behavior, market trends, and overall performance. The robustness and efficiency of the Data Layer are pivotal in maintaining the accuracy and consistency of data, ultimately influencing the effectiveness of decision-making processes and enhancing the overall performance of e-commerce operations. The following concepts are important here.

Database: The data layer stores and manages structured data related to products, customers, orders, and other relevant information. Relational databases or NoSQL databases are commonly used to handle the data storage requirements of e-commerce platforms.

Data Warehousing and Analytics: This component is responsible for collecting and analyzing data to derive insights into customer behavior, sales patterns, and other key metrics. It supports decision-making and helps optimize various aspects of the e-commerce business.

2.4. Integration Layer

The integration layer in e-commerce serves as the connective tissue that links various components and external services, ensuring the seamless flow of information and transactions across the entire system [27]. It encompasses crucial integrations such as payment gateways, enabling secure and efficient financial transactions, and shipping and logistics systems for streamlined order fulfillment. Third-party integrations with services like customer relationship management (CRM) and inventory management further enhance the functionality of the e-commerce platform. This layer plays a key role in orchestrating the collaboration between different components, fostering interoperability, and allowing businesses to leverage a diverse ecosystem of tools and services to optimize their operations and enhance the overall customer experience. *Payment gateway*, *shipping and logistics integration* as well as *third-party integrations* are significant in this domain.

- *Payment Gateway*: Facilitates secure online transactions by connecting the e-commerce platform with payment processors. It ensures that financial transactions are processed securely.
- *Shipping and Logistics Integration*: Connects with shipping carriers and logistics systems to manage order fulfillment, shipping, and tracking.
- *Third-Party Integrations*: E-commerce platforms often integrate with external services such as customer relationship management (CRM), marketing tools, and inventory management systems.

2.5. Security Layer

The security layer in e-commerce is a paramount component focused on safeguarding sensitive information and ensuring the trustworthiness of online transactions. Authentication and authorization mechanisms are implemented to secure user access, protecting customer accounts from unauthorized activities [28]-[30]. SSL/TLS encryption is employed to encrypt data transmitted between users and the e-commerce server, safeguarding personal and financial information during online transactions. Security measures extend to secure payment gateways that handle financial transactions, mitigating the risk of fraud. Robust security practices within this layer are crucial to instill confidence in customers, protect against cyber threats such as data breaches, and uphold the integrity and confidentiality of user data, contributing to the overall trustworthiness of the e-commerce platform. The following concepts are of great importance in this perspective.

- *Authentication and Authorization*: Ensures secure access to the platform, with mechanisms for user authentication and authorization. This layer is crucial for protecting customer data and maintaining the integrity of the e-commerce system.
- *SSL/TLS Encryption*: SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security) are cryptographic protocols designed to secure communications over a computer network, most commonly the internet. They encrypt data transmitted between the user's device and the e-commerce server, safeguarding sensitive information during online transactions as shown in Figure 3.

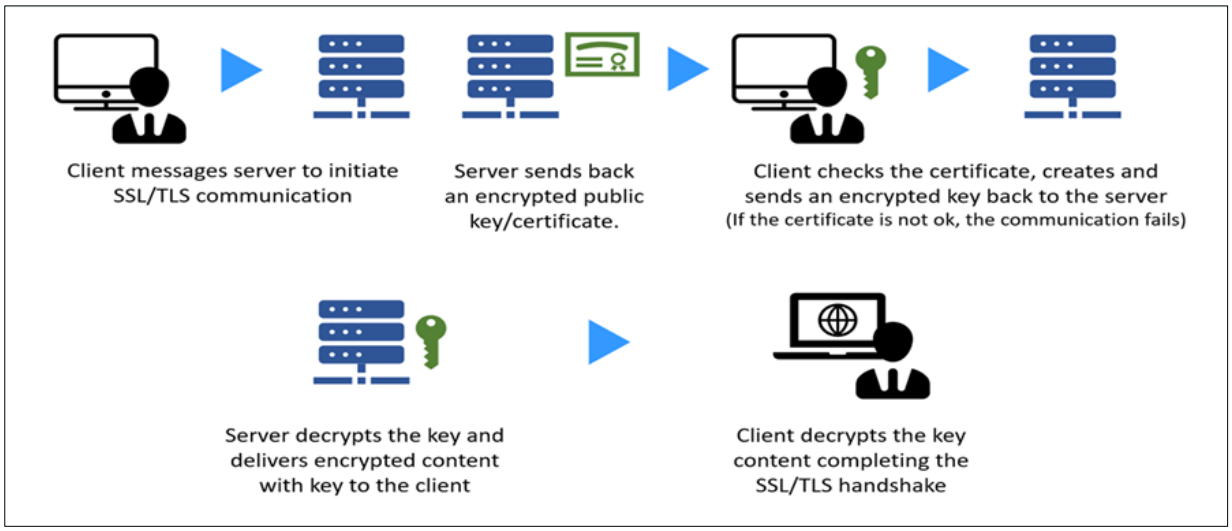

Figure 3 Data protection using SSL/TLS

These protocols establish a secure and encrypted connection between a client and a server, ensuring the confidentiality and integrity of data exchanged between them. SSL/TLS use a combination of asymmetric and symmetric encryption to protect sensitive information from eavesdropping and tampering [31]-[35]. The protocols also involve a handshake process during connection establishment, where the parties authenticate each other and negotiate encryption parameters. SSL/TLS are widely employed to secure online transactions, sensitive data transmissions, and communication between web browsers and servers, offering a crucial layer of security in the digital realm.

2.6. Infrastructure Layer

The infrastructure layer in e-commerce constitutes the foundational technology components that support the overall operation of online platforms. Web servers and application servers host and process the e-commerce application, ensuring its availability and responsiveness to user requests [36]. Load balancers distribute incoming web traffic across multiple servers, optimizing performance and reliability. Cloud services are frequently leveraged to provide scalability, flexibility, and cost efficiency, allowing businesses to adapt to varying demand levels. Together, these components form the backbone of the e-commerce infrastructure, supporting the seamless functioning of the entire system and contributing to the overall reliability and performance of the online platform. The following are quite vital in this perspective. The following concepts are very crucial in this perspective.

- *Web Servers and Application Servers*: Host the e-commerce application and handle user requests.
- *Load Balancers*: Distribute incoming web traffic across multiple servers to ensure optimal performance and reliability.
- *Cloud Services*: Many e-commerce platforms leverage cloud services for scalability, flexibility, and cost efficiency.

2.7. Monitoring and Analytics

Monitoring and analytics in e-commerce are crucial components that provide insights into the performance, user behavior, and overall health of the online platform [37]. As shown in Figure 4, logging and monitoring tools track system performance, detect issues, and log events for analysis, ensuring the stability and reliability of the e-commerce system. Analytics tools delve into vast datasets to uncover valuable information about customer preferences, purchasing patterns, and the effectiveness of marketing strategies.

These insights empower businesses to make data-driven decisions, refine their approach to user engagement, optimize pricing strategies, and enhance overall operational efficiency [40]. By continuously monitoring and analyzing key metrics, e-commerce businesses can adapt to market dynamics and continually improve the user experience, contributing to the long-term success and growth of the online platform. *Analytics tools*, *logging and monitoring tools* are key concepts in this perspective.

- *Logging and Monitoring Tools*: Track system performance, detect issues [41], and log events for analysis.
- *Analytics Tools*: Provide insights into user behavior, traffic patterns, and overall platform performance.

Figure 4 Monitoring and analytics in e-commerce

Ideally, e-commerce architecture can vary based on the scale and specific requirements of the business. Whether it's a small online store or a large-scale enterprise platform, a well-designed architecture is essential for the seamless operation and growth of e-commerce businesses.

3. E-commerce merits

E-commerce, or electronic commerce, has brought about a paradigm shift in the way businesses operate and consumers engage in commerce, offering a multitude of merits that span various dimensions of the business landscape [42]. Table 1 below summarizes the strengths of e-commerce transactions.

Table 1 Merits of e-commerce

Merit	Description
Global reach	Perhaps one of the most significant merits of e-commerce is its ability to transcend geographical boundaries, enabling businesses to reach a global audience [43]. This global reach opens up new markets and customer segments, providing businesses with unprecedented opportunities for expansion.
Convenience and accessibility	E-commerce provides unparalleled convenience for consumers, allowing them to shop 24/7 from anywhere with an internet connection [44]. This accessibility eliminates the constraints of traditional brick-and-mortar store hours, making it convenient for customers to browse, compare products, and make purchases at their convenience.
Cost efficiency	For businesses, e-commerce often translates into cost savings. The need for physical storefronts is reduced or eliminated, lowering expenses related to rent, utilities, and maintenance [45]. This cost efficiency can be particularly advantageous for small and medium-sized enterprises (SMEs) looking to establish an online presence without the financial burden of maintaining a physical location.
Data-driven decision-making	E-commerce platforms generate vast amounts of data, offering valuable insights into customer behavior, preferences, and market trends [46]. Businesses can leverage analytics to make data-driven decisions, refine marketing strategies, optimize pricing, and enhance overall operational efficiency.
Scalability	E-commerce platforms provide scalability, allowing businesses to easily expand their operations as demand grows [47]. Whether it's increasing product offerings, expanding into new markets, or accommodating a larger customer base, e-commerce provides the flexibility to scale operations efficiently.

Personalization	E-commerce allows for highly personalized customer experiences. Through data analysis and artificial intelligence [48], businesses can tailor recommendations, promotions, and content to individual customer preferences, increasing the likelihood of conversion and fostering customer loyalty.
Innovation and technology integration	E-commerce encourages innovation by providing a platform for the integration of cutting-edge technologies. Augmented reality for virtual try-ons, artificial intelligence for personalized recommendations, and chatbots for customer support are just a few examples of how technology enhances the e-commerce experience [49]-[54].
Accessibility for small businesses	E-commerce levels the playing field for small businesses, enabling them to compete with larger enterprises [55]. The online marketplace allows small businesses to showcase their products or services to a global audience without the need for a physical presence in multiple locations.
Reduced time to market	Traditional retail processes often involve lengthy supply chains and distribution channels. E-commerce streamlines these processes, reducing the time it takes for products to go from production to the hands of the consumer [56]. This agility is crucial in responding to rapidly changing market demands.
Environmental impact	In some cases, e-commerce can have a lower environmental impact compared to traditional retail. By reducing the need for physical stores and optimizing supply chain processes, e-commerce can contribute to lower carbon footprints and more sustainable business practices [57].

Evidently, the merits of e-commerce extend beyond mere convenience, encompassing cost savings, global reach, data-driven insights, and the ability to create highly personalized customer experiences. As technology continues to advance, the benefits of e-commerce are likely to evolve, presenting new opportunities for businesses to thrive in the digital era.

4. Privacy issues in E-commerce

Privacy issues in e-commerce are pervasive and multifaceted, primarily centered around the extensive collection and handling of personal information by online retailers [58], [59]. E-commerce platforms routinely gather sensitive data [60], including names, addresses, and payment details, raising concerns about the security and responsible use of this information. Instances of data breaches pose a significant threat, as cybercriminals target e-commerce sites to exploit the wealth of personal and financial data stored, potentially leading to identity theft and financial losses for consumers. Figure 5 presents some of the most common threats in e-commerce environment.

Moreover, the pervasive use of cookies and tracking technologies for user behavior analysis raises questions about the transparency of such practices, as users may not be fully aware of the extent to which their activities are monitored and how this information is utilized by both the e-commerce platform and third-party entities. According to [61], privacy issues in e-commerce have become increasingly significant as online shopping continues to grow in popularity. Here are several aspects to consider when discussing privacy issues in the context of e-commerce:

4.1. Data Collection and Storage

E-commerce platforms often collect a vast amount of personal information, including names, addresses, phone numbers, and payment details. The gathering of such data raises concerns about how it will be used and stored [62]. In addition, many e-commerce sites use cookies and tracking technologies to monitor user behavior [63]. While this can enhance the shopping experience, it also raises privacy concerns, as users may not be fully aware of the extent of tracking.

To address cookies and tracking threats in e-commerce, businesses can implement a combination of technical measures and transparent privacy practices. First, providing users with clear and easily accessible information about the types of cookies used, their purposes, and the option to opt-out enhances transparency and builds trust. Implementing robust cookie management tools allows users to control their cookie preferences. Moreover, adopting secure and privacy-focused technologies such as HTTP Secure (HTTPS) ensures encrypted data transmission, reducing the risk of interception by malicious entities [64]-[66]. Regular security audits and updates to address vulnerabilities in tracking mechanisms are also essential. By prioritizing user privacy, offering transparency, and employing secure technologies, e-commerce platforms can strike a balance between personalized user experiences and safeguarding customer privacy.

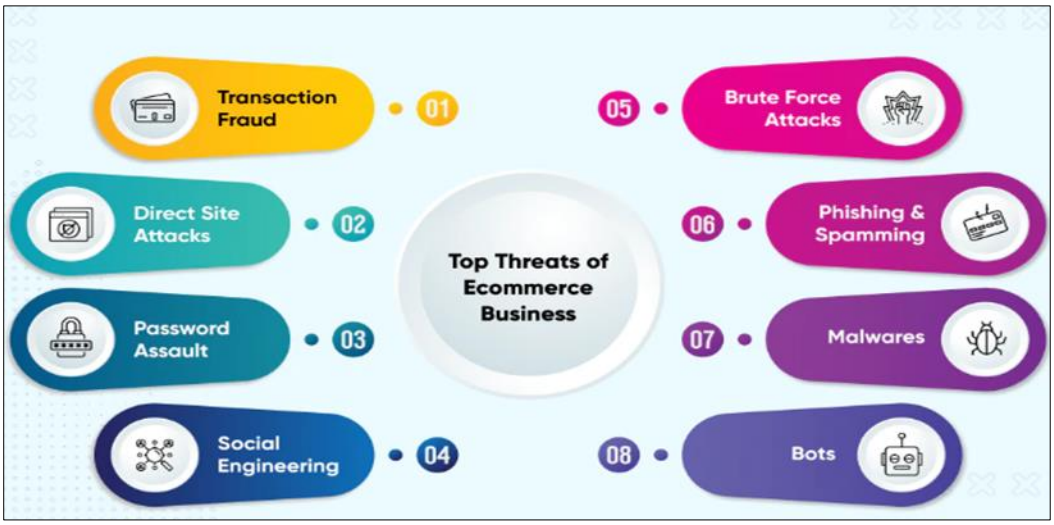

Figure 5 Common threats in e-commerce

4.2. Third-Party Involvement

E-commerce businesses often collaborate with third-party service providers, such as marketing analytics, advertising, and logistics companies [67], [68]. Customers may be unaware of the extent to which their data is shared with these third parties, raising concerns about data ownership and control. In addition, e-commerce platforms should have clear and transparent privacy policies that detail how customer data is handled, shared, and protected [69]-[72]. However, these policies are often lengthy and complex, leading to challenges for users in understanding them fully.

To mitigate third-party involvement threats in e-commerce, businesses should conduct thorough due diligence when selecting and integrating third-party services, such as payment processors and external plugins. Regular security assessments and audits of third-party providers can help identify vulnerabilities and ensure they adhere to robust security practices [73], [74]. Implementing strict access controls and monitoring mechanisms to restrict the privileges of third-party entities reduces the risk of unauthorized access and data breaches. Additionally, businesses should stay informed about the security practices of their third-party partners and promptly address any reported vulnerabilities. By actively managing and securing third-party relationships, e-commerce platforms can bolster their overall security posture and minimize the potential impact of external threats on customer data and transactions.

4.3. User Consent and Control

Customers should have the option to opt in or opt out of data collection and marketing communications [75]. However, some platforms may default to opt-in, requiring users to actively seek opt-out options. In addition, e-commerce sites should provide users with control over their personal information [76]. This includes the ability to update, edit, or delete their data, as well as controlling preferences for marketing communications.

To address user consent and control threats in e-commerce, businesses should prioritize transparency and user empowerment. Implementing clear and user-friendly privacy policies that detail the types of data collected, its purpose, and how it will be used, ensures that customers are well-informed about data practices [77]. Providing granular consent options enables users to choose the level of information they are comfortable sharing. Robust preference management tools, allowing users to easily adjust their privacy settings, contribute to a sense of control over their data. Regularly updating and communicating privacy policies in response to changes in data practices or regulations demonstrates a commitment to user-centric privacy. By empowering users with informed choices and control over their data, e-commerce platforms can build trust and foster a more secure and privacy-respecting online environment.

4.4. Emerging Technologies

While AI [78] can enhance the personalization of the shopping experience, it also raises concerns about how customer data is used to make decisions. There is a fine line between helpful recommendations and invasive data usage [79], [80]. Some e-commerce platforms may use biometric data, such as fingerprints or facial recognition, for authentication. The collection and storage of such sensitive data require robust security measures and clear consent from users [81].

To address threats associated with the collection and storage of sensitive data in e-commerce, businesses should prioritize data minimization, encryption, and secure storage practices. Implementing a policy of only collecting the minimum necessary data for transactional purposes reduces the volume of sensitive information stored, limiting potential exposure. Utilizing strong encryption protocols, both during data transmission and while at rest in storage, helps safeguard sensitive information from unauthorized access. Secure storage mechanisms, including regularly updated security patches and access controls, protect against data breaches and ensure compliance with data protection regulations [82], [83]. Additionally, adopting tokenization or pseudonymization techniques can further enhance data security by replacing sensitive information with non-sensitive equivalents. By adopting a comprehensive approach to data security that encompasses minimization, encryption, secure storage, and regulatory compliance, e-commerce platforms can significantly mitigate the risks associated with the handling of sensitive customer information.

4.5. Global Compliance and Regulations

E-commerce businesses must comply with data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union [84]. Understanding and adhering to these regulations can be challenging, especially for global e-commerce platforms that operate in multiple jurisdictions with varying privacy laws. E-commerce platforms can achieve compliance with the General Data Protection Regulation (GDPR) and other relevant regulations by implementing a comprehensive data protection strategy. This includes obtaining explicit consent from users before collecting and processing their personal data, providing transparent privacy policies, and offering users the right to access, correct, and delete their information. Implementing robust security measures, such as encryption and regular security audits, ensures the confidentiality and integrity of customer data. E-commerce businesses should appoint a Data Protection Officer (DPO) to oversee compliance efforts, conduct privacy impact assessments, and establish protocols for reporting data breaches [85], [86]. Regular employee training on data protection principles and practices is crucial, and contractual agreements with third-party vendors should include provisions for data protection. By adopting a privacy-by-design approach and staying informed about evolving regulations, e-commerce platforms can build and maintain trust with customers while meeting legal obligations.

Therefore, addressing privacy issues in e-commerce requires a comprehensive approach that combines technological safeguards, clear communication, and adherence to relevant regulations. As e-commerce continues to evolve, it's crucial for businesses to prioritize user privacy to build trust and maintain a positive relationship with their customers [87]-[89]. In addition, e-commerce businesses must prioritize security measures, implement transparent privacy policies, and empower users with control over their data. Clear communication about data usage, robust encryption protocols for secure transactions, and adherence to data protection regulations like GDPR are essential elements for establishing and maintaining trust with consumers. Striking a balance between personalization for an enhanced shopping experience and safeguarding user privacy remains a critical challenge for e-commerce platforms as they navigate the evolving landscape of online retail. Table 2 presents some notable incidents involving privacy breaches in the e-commerce sector.

Table 2 Notable e-commerce privacy leaks

Incident	Year	Description
Target	2013	One of the most infamous breaches, Target experienced a massive data breach during the holiday season, affecting millions of customers' credit and debit card information.
eBay	2014	In 2014, eBay faced a significant breach compromising personal information, including passwords, of around 145 million users.
Equifax	2017	While not an e-commerce platform per se, Equifax, a credit reporting agency, suffered a major data breach, exposing sensitive personal information of millions, impacting online financial transactions and e-commerce activities.
Yahoo	2013-2014	Yahoo experienced a series of breaches affecting billions of user accounts, including email accounts linked to e-commerce platforms.
Home Depot	2014	Home Depot encountered a data breach that exposed credit card information of millions of customers, impacting those who made purchases online and in-store.
Under Armour's MyFitnessPal	2018	While not a traditional e-commerce platform, MyFitnessPal's data breach affected users who often link their fitness apps to e-commerce sites, potentially revealing personal information and habits.

Amazon Ring	2019	Ring, a subsidiary of Amazon, faced privacy concerns related to unauthorized access to users' cameras and personal information, raising questions about the security of smart home devices.
Wish	2020	Wish, a popular online marketplace, faced criticism for privacy issues related to the collection and handling of user data, including concerns about sharing data with third-party advertisers.
EasyJet	2020	While not strictly an e-commerce platform, the airline EasyJet experienced a data breach that exposed personal information of millions of customers, including those who may have booked flights online.

These incidents highlight the importance of robust cybersecurity measures and the need for constant vigilance to protect user privacy in the e-commerce sector. It's crucial for businesses to continually update and enhance their security practices to stay ahead of evolving cyber threats [90].

5. Security issues in E-commerce

Security issues in e-commerce pose substantial challenges due to the sensitive nature of the data involved in online transactions. One prominent concern is the prevalence of data breaches, where malicious actors exploit vulnerabilities in e-commerce platforms to gain unauthorized access to customer information [91]-[94]. These breaches can result in the exposure of personal details, payment data, and login credentials, leading to severe consequences such as identity theft and financial fraud for affected users. The frequency and sophistication of cyber-attacks targeting e-commerce sites underline the critical need for robust security measures, including regular security audits, encryption protocols, and secure payment gateways, to safeguard customer information from unauthorized access and prevent data breaches.

Additionally, the emergence of new technologies in e-commerce introduces novel security considerations [95], [96]. As more businesses adopt artificial intelligence and machine learning for tasks like fraud detection and personalization, it becomes imperative to ensure that these technologies are implemented securely. Biometric authentication methods, such as fingerprint or facial recognition, add another layer of complexity, requiring stringent security protocols to protect the biometric data collected [97]-[99]. In addressing security issues in e-commerce, a comprehensive approach involving continual monitoring, regular updates to security infrastructure, and user education about best security practices is crucial to building and maintaining trust among online shoppers. Figure 6 demonstrates how secure communication can be achieved in an e-commerce environment. According to [100], security is a critical aspect of e-commerce, as it involves the online transaction of sensitive information such as personal and financial data. Various security issues can arise in the e-commerce environment, and addressing these concerns is essential to build trust among consumers. Here are some key security issues in e-commerce:

5.1. Data Breaches

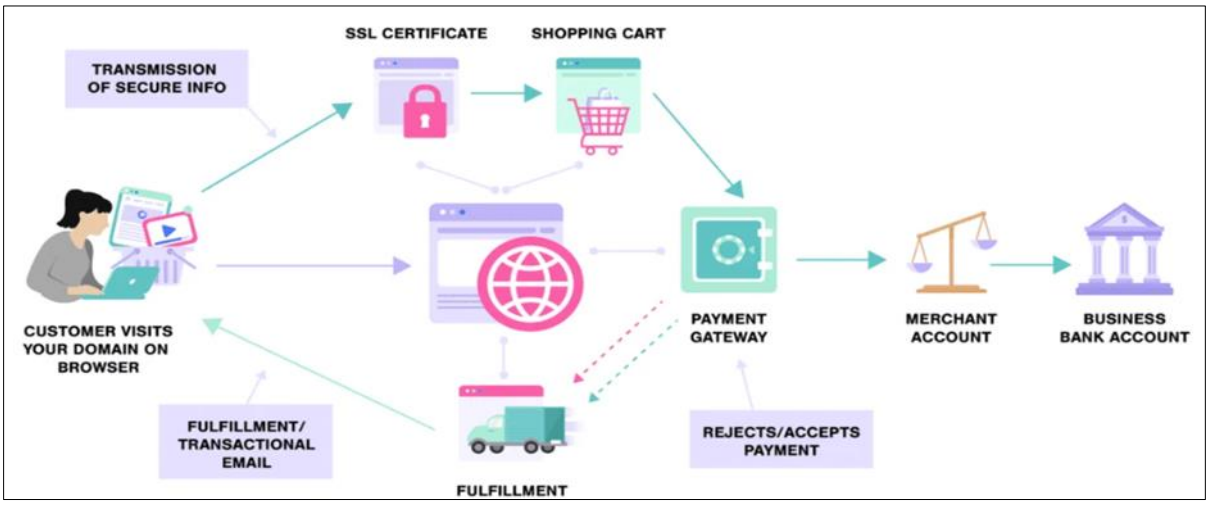

Figure 6 Secure communication in e-commerce

Data breaches involve unauthorized access to a system or network, resulting in the theft of sensitive information [101]. Data breaches in e-commerce represent a significant and pervasive threat to both businesses and consumers. These breaches typically involve the unauthorized access to sensitive customer information, including personal details and financial data. The impact of a data breach can be severe, leading to compromised customer trust, financial losses, and damage to the affected company's reputation [102]-[104].

Cybercriminals often target e-commerce platforms to harvest large amounts of valuable data, which can be sold on the dark web or used for various malicious activities such as identity theft and fraudulent transactions. As e-commerce relies heavily on the exchange of personal and financial information during transactions, the occurrence of a data breach can have far-reaching consequences, affecting not only the immediate victims but also eroding the overall confidence in online shopping platforms.

- **Impact:** Customer data, including personal and financial details, can be exposed, leading to identity theft and financial fraud.
- **Mitigation:** to alleviate the risks associated with data breaches, e-commerce businesses must prioritize robust cybersecurity measures. This includes implementing strong encryption protocols to protect data both in transit and at rest, ensuring secure authentication methods, regularly conducting security audits, and staying vigilant against emerging threats [105-[109]. Additionally, prompt and transparent communication with affected parties in the event of a breach is crucial for rebuilding trust. Proactive monitoring, threat intelligence, and adherence to industry compliance standards further contribute to creating a resilient defense against the evolving landscape of cyber threats in the e-commerce sector.

5.2. Payment Card Fraud

Criminals may use stolen credit card information to make unauthorized purchases. Payment card fraud is a prevalent and persistent challenge in the realm of e-commerce, posing significant risks to both consumers and businesses [110], [111]. Criminals exploit vulnerabilities in the online payment process to gain unauthorized access to credit card information, subsequently using these details to make fraudulent transactions. The nature of e-commerce, where customers input their payment information for online purchases, makes it a prime target for payment card fraud. Fraudulent activities can range from unauthorized transactions and account takeovers to the creation of counterfeit cards. The financial repercussions for businesses include chargeback fees, lost revenue, and potential damage to the brand's reputation. For consumers, the aftermath may involve identity theft, financial losses, and the arduous process of reclaiming their funds and resecuring their accounts.

- **Impact:** Businesses may face financial losses, and consumers may experience fraudulent charges on their credit cards.
- **Mitigation:** to combat payment card fraud in e-commerce, robust security measures are essential. Implementation of secure and PCI DSS (Payment Card Industry Data Security Standard) compliant payment gateways, tokenization of card data, and two-factor authentication are crucial steps [112]-[114]. Regular monitoring for suspicious activities, real-time fraud detection systems, and collaboration with payment networks and financial institutions contribute to early detection and prevention of fraudulent transactions. E-commerce businesses also need to prioritize customer education on safe online practices, including recognizing phishing attempts [115] and regularly monitoring their financial statements for any unauthorized transactions. The collaborative efforts of technology, regulation, and user awareness are vital in building a resilient defense against the ever-evolving landscape of payment card fraud in e-commerce.

5.3. Phishing Attacks

Phishing involves tricking individuals into providing sensitive information by posing as a trustworthy entity [117]. Payment card fraud is a prevalent and persistent challenge in the realm of e-commerce, posing significant risks to both consumers and businesses. Criminals exploit vulnerabilities in the online payment process to gain unauthorized access to credit card information, subsequently using these details to make fraudulent transactions [118], [119]. The nature of e-commerce, where customers input their payment information for online purchases, makes it a prime target for payment card fraud.

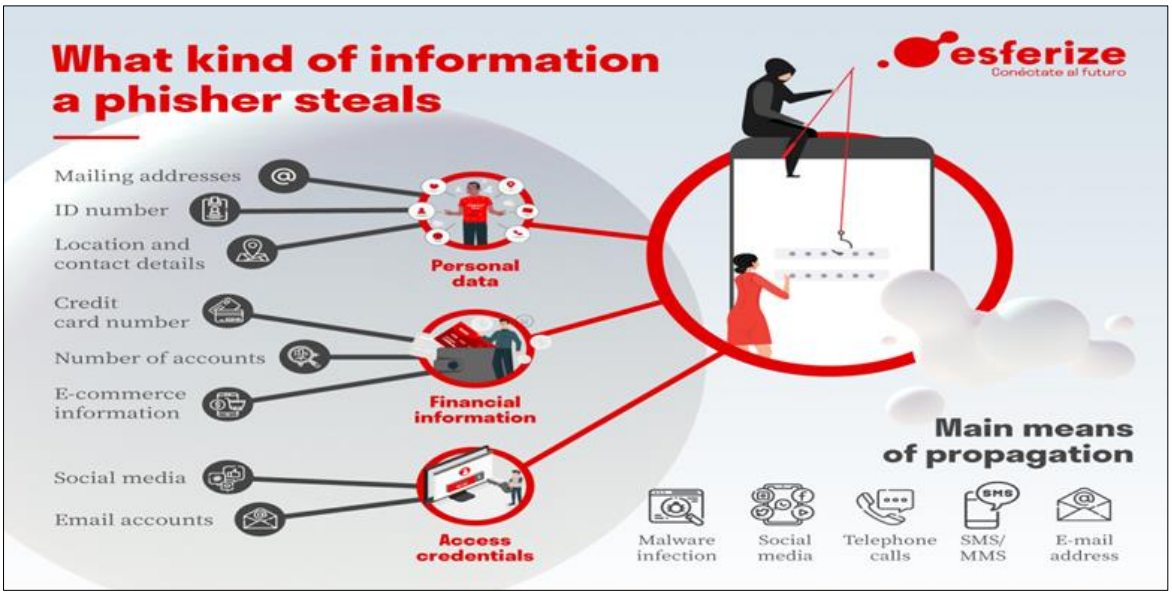

Figure 7 Phishing in e-commerce

Fraudulent activities can range from unauthorized transactions and account takeovers to the creation of counterfeit cards. The financial repercussions for businesses include chargeback fees, lost revenue, and potential damage to the brand's reputation. For consumers, the aftermath may involve identity theft, financial losses, and the arduous process of reclaiming their funds and resecuring their accounts.

- **Impact:** Consumers and employees may unknowingly disclose usernames, passwords, or other confidential information, leading to unauthorized access.
- **Mitigation:** to prevent phishing attacks in e-commerce, implementing a multi-layered security approach is crucial. Firstly, educate both customers and employees about the risks associated with phishing, emphasizing the importance of verifying email and website authenticity. Employ email authentication protocols [120] such as DMARC to detect and prevent email spoofing. Implement robust SSL encryption for secure data transmission and ensure that your e-commerce platform is regularly updated with the latest security patches. Utilize advanced threat detection tools to identify and block phishing attempts in real-time, and employ two-factor authentication for an additional layer of user verification [121], [122]. Regularly audit and monitor website logs for suspicious activities, and promptly address any reported phishing incidents. Finally, foster a security-conscious culture within the organization to promote vigilance and proactive responses to emerging threats.

5.4. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

These attacks overwhelm a system or network with traffic, causing it to become slow or unavailable. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks represent significant threats to the availability and functionality of e-commerce websites [123]-[126]. In a DoS attack, malicious actors attempt to overwhelm a target website or online service by flooding it with an excessive volume of traffic, rendering it slow or completely unavailable to legitimate users. Figure 8 presents an illustration of a typical DoS/DDoS.

DDoS attacks, on the other hand, involve the coordination of multiple compromised devices (often part of a botnet) to amplify the scale of the attack. E-commerce platforms are particularly vulnerable to these attacks as any disruption in service can result in financial losses, damage to brand reputation, and a decline in customer trust [127], [128]. Attackers may launch DoS or DDoS attacks to extort money, settle personal vendettas, or simply disrupt business operations for competitive reasons.

- **Impact:** E-commerce websites may experience downtime, leading to loss of revenue and damage to the brand's reputation.
- **Mitigation:** to defend against DoS and DDoS attacks, e-commerce businesses need to implement robust security measures. This includes deploying dedicated DDoS mitigation tools and services that can identify and filter out malicious traffic while allowing legitimate users to access the website seamlessly [129], [130]. Cloud-based DDoS protection services, which leverage the scalability of cloud infrastructure, are often employed to

absorb and mitigate large-scale attacks. Additionally, having a comprehensive incident response plan and a well-defined communication strategy can help e-commerce businesses minimize the impact of such attacks and quickly restore normal operations. Regular testing of defense mechanisms, continuous monitoring, and collaboration with DDoS mitigation experts can enhance the overall resilience of e-commerce platforms against these disruptive threats.

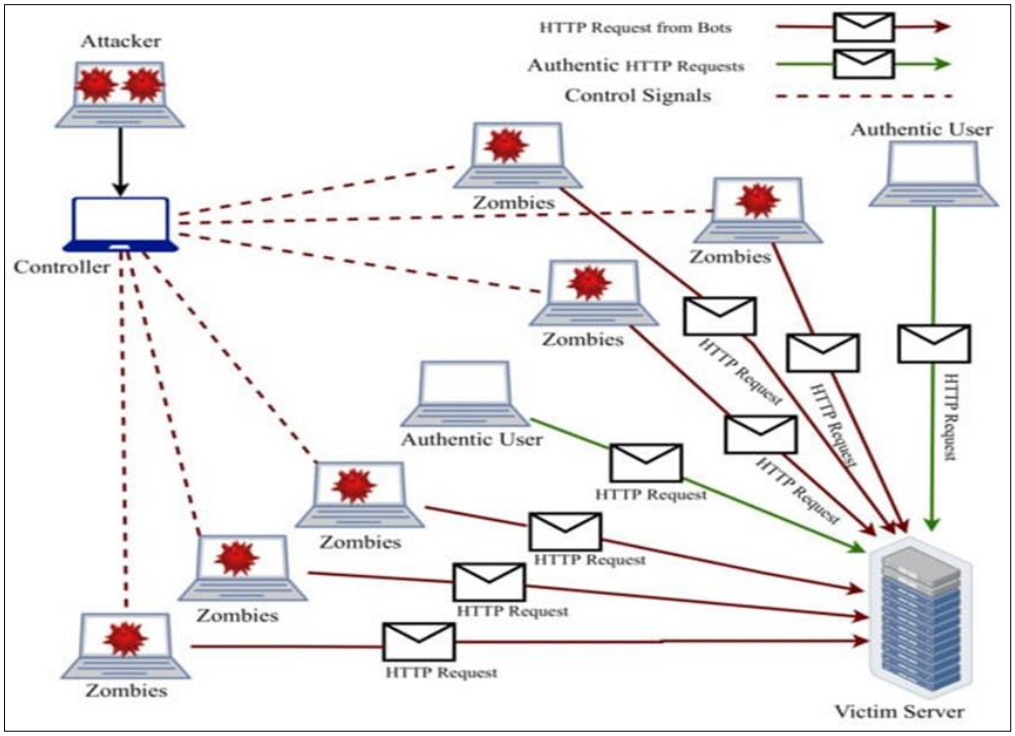

Figure 8 DDoS and DoS attacks

5.5. Insecure Payment Gateways

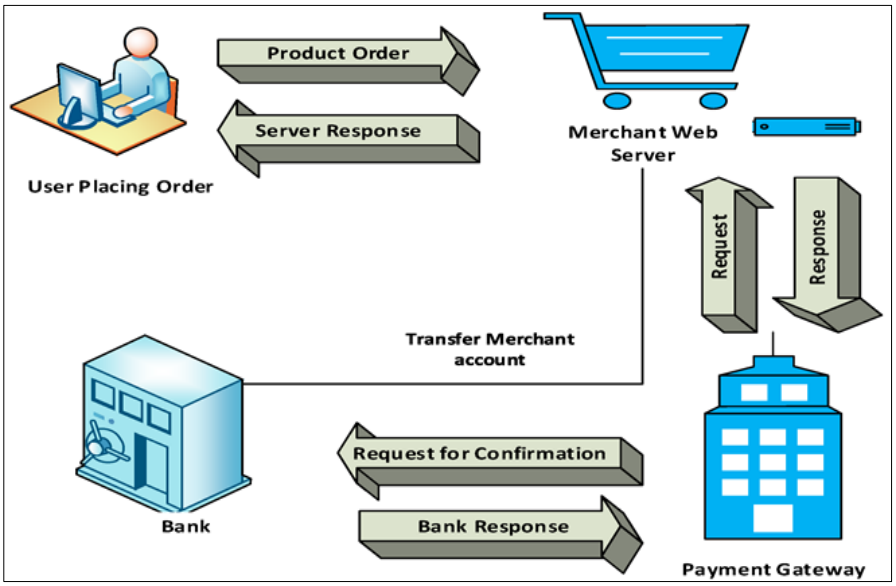

Figure 9 Payment gateways in e-commerce

Weaknesses in the payment processing system can be exploited to intercept and manipulate transactions [131]. Figure 9 shows a typical payment system through the payment gateway. Payment gateways serve as the interface between a merchant's website and the payment processing networks, facilitating the secure transmission of sensitive payment

information. Insecure payment gateways pose a significant risk to the integrity and confidentiality [132] of financial transactions in e-commerce. If these gateways are inadequately secured, malicious actors can exploit vulnerabilities to intercept and manipulate transaction data, leading to unauthorized access and potential compromise of customer financial details.

Insecure payment gateways may result from poor coding practices, lack of encryption, or insufficient authentication protocols, providing a potential entry point for attackers seeking to compromise the payment process [133]-[136].

- **Impact:** Financial information may be compromised, leading to fraudulent transactions and financial losses.
- **Mitigation:** reduction of the risks associated with insecure payment gateways involves implementing robust security measures throughout the entire payment processing lifecycle. This includes deploying end-to-end encryption [137] to protect the confidentiality of data during transmission, adopting industry-standard encryption protocols such as SSL/TLS, and ensuring compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements [138], [139]. Regular security audits, vulnerability assessments, and penetration testing can help identify and address potential weaknesses in payment gateway systems. E-commerce businesses must prioritize the selection of reputable and secure payment gateway providers and stay informed about emerging threats and best practices in the constantly evolving landscape of online payment security. By proactively addressing vulnerabilities in payment gateways, businesses can safeguard customer trust, protect financial transactions, and maintain the overall security of their e-commerce platforms.

5.6. Inadequate Authentication and Authorization

Weak authentication mechanisms or insufficient authorization processes can lead to unauthorized access [140]. Inadequate authentication and authorization mechanisms in e-commerce present serious security vulnerabilities, exposing businesses and customers to various risks. Authentication verifies the identity of users accessing an e-commerce platform, while authorization ensures that users have the appropriate permissions to perform specific actions. Weak authentication, such as the use of easily guessable passwords or the absence of multi-factor authentication, can leave user accounts susceptible to unauthorized access [141]-[143]. Similarly, insufficient authorization controls may grant users more privileges than necessary, providing opportunities for attackers to exploit elevated access rights and compromise sensitive data, manipulate transactions, or engage in fraudulent activities.

- **Impact:** Attackers may gain access to sensitive data, manipulate transactions, or compromise user accounts.
- **Mitigation:** to enhance security, e-commerce platforms must implement strong authentication practices and robust authorization controls. This involves encouraging users to employ complex passwords, enforcing multi-factor authentication, and regularly updating access credentials. Role-based access controls should be established to limit user permissions based on their roles within the organization, ensuring that individuals only have access to the resources necessary for their duties [144]-[149]. Regular security audits and monitoring of user activities are essential to promptly identify and address any anomalies or unauthorized access attempts. By prioritizing strong authentication and authorization practices, e-commerce businesses can significantly reduce the risk of unauthorized access and protect both customer information and their own sensitive data.

5.7. Insufficient Encryption

Failure to encrypt data during transmission and storage can expose sensitive information to interception [150]. Insufficient encryption in e-commerce transactions poses a grave threat to the confidentiality and integrity of sensitive data exchanged between customers and businesses. Encryption is a fundamental security measure that transforms data into unreadable, scrambled formats during transmission, safeguarding it from interception by malicious actors. Inadequate encryption practices, such as using weak encryption algorithms or neglecting to encrypt specific types of data, expose customer information, including personal details and payment credentials, to potential eavesdropping and unauthorized access [151]-[155]. Cybercriminals often target these vulnerabilities to intercept and exploit the unsecured data, leading to financial fraud, identity theft, and compromise of sensitive customer information.

- **Impact:** Unencrypted data is vulnerable to eavesdropping, leading to the compromise of sensitive information.
- **Mitigation:** to bolster security in e-commerce, robust encryption practices must be implemented across the entire data lifecycle. This includes encrypting data during transmission through the use of secure protocols like SSL/TLS, as well as encrypting data at rest within databases or storage systems. Regularly updating encryption protocols to adhere to industry best practices and compliance standards, such as Payment Card Industry Data Security Standard (PCI DSS), is imperative [156]-[159]. E-commerce businesses should also educate their customers about the importance of encryption and reassure them that their sensitive information is adequately protected. By prioritizing

and maintaining strong encryption measures [16-], e-commerce platforms can instill trust among customers and fortify their defense against potential cyber threats.

6. Unsecure APIs

Insecure Application Programming Interfaces (APIs) can be exploited to gain unauthorized access or manipulate data [161]. Unsecured Application Programming Interfaces (APIs) in e-commerce introduce significant vulnerabilities that can be exploited by malicious actors to compromise the integrity and confidentiality of sensitive data. APIs facilitate the seamless exchange of information between different software components, enabling functionalities such as payment processing and order fulfillment in e-commerce platforms. However, if these APIs lack robust security measures, they become potential entry points for attackers. Unsecured APIs may be susceptible to various threats, including unauthorized access, data manipulation, and injection attacks [162]-[164]. Cybercriminals can exploit weaknesses in API design, inadequate authentication mechanisms, or insufficient encryption, allowing them to gain unauthorized access to critical systems, manipulate transactions, and compromise user data.

- **Impact:** Attackers may compromise the integrity of transactions or access sensitive information through vulnerable APIs.
- **Mitigation:** to allay the risks associated with unsecured APIs, e-commerce businesses must prioritize the implementation of robust security measures. This includes enforcing proper authentication protocols [165], such as API keys or OAuth tokens, to ensure that only authorized entities can access the APIs. Employing encryption for data transmitted via APIs and regularly monitoring and auditing API activity are essential practices. Additionally, keeping APIs updated with the latest security patches and adhering to industry standards and best practices can significantly enhance the overall security posture of e-commerce platforms [166], [167]. By securing APIs, businesses not only protect their own systems and data but also contribute to a safer and more trustworthy online shopping environment for their customers.

6.1. Poorly Configured Security Settings

Improperly configured security settings, such as weak passwords or lax access controls, can create vulnerabilities [168]. Poorly configured security settings in e-commerce platforms expose businesses to significant risks, as they create vulnerabilities that can be exploited by malicious actors. These settings encompass a wide range of parameters, including weak passwords, lax access controls, and improperly configured firewalls. Weak passwords, often resulting from a lack of password complexity requirements or infrequent password updates, make it easier for attackers to gain unauthorized access to sensitive systems. Similarly, lax access controls may grant unnecessary permissions to users, increasing the likelihood of unauthorized individuals exploiting these privileges to compromise confidential data, manipulate transactions, or disrupt business operations [170]-[172]. Inadequate firewall configurations may leave entry points open for cyber threats, allowing malicious actors to exploit vulnerabilities and compromise the security of e-commerce platforms.

- **Impact:** Unauthorized individuals may exploit these settings to gain access to sensitive systems and data.
- **Mitigation:** to bolster security, e-commerce businesses must invest in proper configuration management and regular security audits. This involves implementing strong password policies, enforcing the principle of least privilege to restrict user access to essential functions, and ensuring that firewalls are configured to block unauthorized access while allowing legitimate traffic [173], [174]. Continuous monitoring of system logs and timely response to security incidents are crucial components of an effective security strategy. Regularly updating and patching software and systems further strengthens the overall security posture, as it addresses known vulnerabilities. By proactively addressing poorly configured security settings, e-commerce platforms can significantly reduce the risk of unauthorized access and protect the confidentiality and integrity of sensitive data.

6.2. Lack of Security Awareness

Insufficient awareness and education about security best practices among employees and customers [175]. The lack of security awareness in e-commerce poses a serious threat as it increases the risk of individuals, both consumers and employees, falling victim to various cyber threats. Consumers may be unaware of the potential risks associated with online transactions, making them more susceptible to phishing attacks, fraudulent schemes, and identity theft. They may inadvertently disclose sensitive information, such as login credentials or credit card details, due to a lack of awareness about secure online practices [176], [177]. On the business side, employees who are not adequately trained in cybersecurity may unknowingly engage in risky behaviors, such as clicking on malicious links or neglecting security protocols, which could expose the organization to data breaches or other security incidents.

- **Impact:** Users may fall victim to social engineering attacks, increasing the risk of security breaches.
- **Mitigation:** to address the lack of security awareness in e-commerce, businesses must prioritize comprehensive education and training programs. Consumer awareness campaigns can inform users about common cyber threats, teach them how to recognize phishing attempts, and encourage the use of secure practices, such as regularly updating passwords and monitoring financial statements. Internally, e-commerce companies should conduct regular security training for employees, covering topics like secure coding practices, the importance of strong authentication, and the potential risks associated with social engineering attacks [178]-[180]. By fostering a culture of security awareness among both customers and employees, e-commerce platforms can significantly reduce the likelihood of successful cyber attacks and contribute to a safer online environment. Figure 10 depicts a secure e-commerce transaction phases.

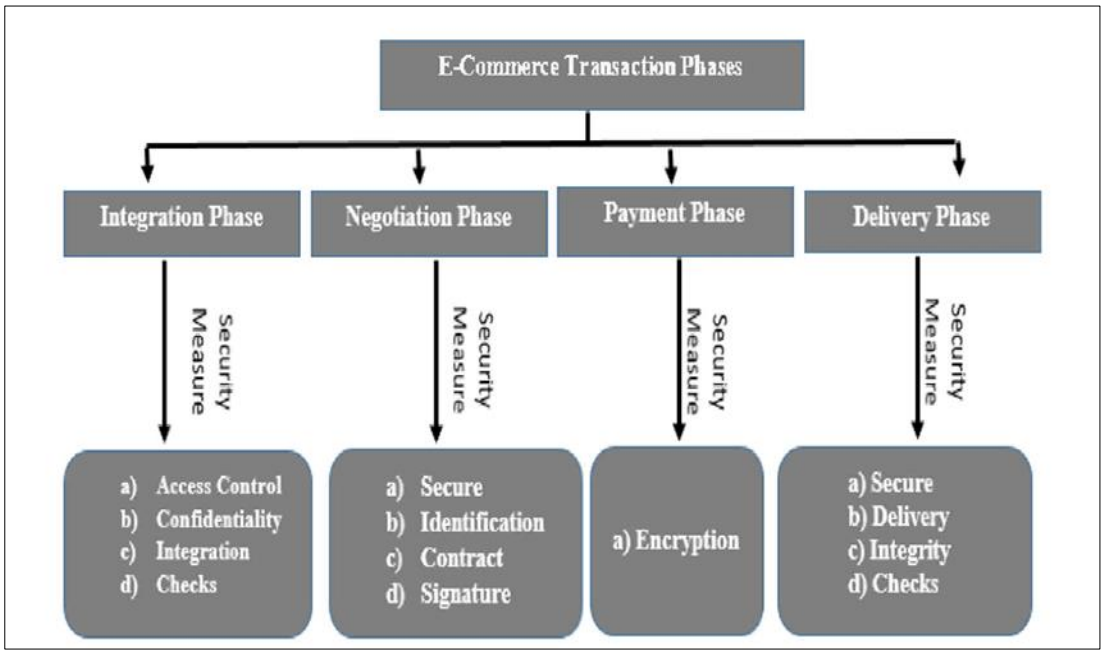

Figure 10 Secure e-commerce transaction phases

It is evident that to address e-commerce security issues, businesses should implement a comprehensive security strategy that includes encryption, secure authentication processes, regular security audits, employee training, and up-to-date security measures. Compliance with industry standards and regulations is also crucial to ensure the protection of customer data. Regular monitoring and prompt response to security incidents are essential components of a robust e-commerce security posture. Some of the notable security incidents in e-commerce are presented in Table 3.

Table 3 Prominent e-commerce security breaches

Incident	Year	Description
Ashley Madison	2015	The Ashley Madison breach exposed user data, including names and email addresses, from the controversial extramarital affairs website.
TalkTalk	2015	The UK-based telecom company TalkTalk faced a cyberattack that exposed customer data, including names, addresses, and financial information.
DYN DNS	2016	The DYN DNS cyberattack disrupted major websites, including e-commerce platforms, through a large-scale Distributed Denial of Service (DDoS) attack.
WannaCry Ransomware	2017	While not specific to e-commerce, the WannaCry ransomware attack affected various sectors, including some e-commerce businesses, encrypting data and demanding ransom payments.
Magecart Attacks	2018-2019	E-commerce websites, including British Airways and Ticketmaster, fell victim to Magecart attacks, compromising payment card information by injecting malicious scripts.

Marriott International	2018	Marriott faced a data breach affecting around 500 million guests, exposing personal information including names, addresses, and passport details.
Quest Diagnostics	2019	A third-party billing collections vendor for Quest Diagnostics suffered a data breach, compromising the personal and financial information of 11.9 million patients.
Capital One	2019	Capital One experienced a data breach where a hacker gained access to the personal information of over 100 million customers, including credit card applications and social security numbers.
Canva	2019	Graphic design tool Canva faced a data breach affecting 139 million users, with exposed information including usernames, email addresses, and encrypted passwords.
Macy's	2019	Macy's suffered a data breach impacting online customers, with unauthorized access leading to the exposure of personal information.
Riviera Beach	2019	The city of Riviera Beach in Florida paid a ransom of $600,000 after a ransomware attack affected its computer systems, highlighting the risks municipalities face.
Canon	2020	Canon experienced a ransomware attack impacting various services, including its online photo and video storage platform.
Blackbaud	2020	Blackbaud, a cloud computing provider for nonprofits, faced a data breach compromising the personal information of millions, including donors of affected organizations.
Molson Coors	2020	Molson Coors fell victim to a cybersecurity incident, disrupting its brewing operations and supply chain.
SolarWinds Supply Chain	2020	While affecting various industries, the SolarWinds cyberattack had implications for e-commerce by compromising the security of organizations that used SolarWinds software.

These incidents underscore the importance of robust cybersecurity measures for e-commerce platforms to protect sensitive customer data and maintain trust in online transactions. It's crucial for businesses to stay informed about evolving threats and continuously enhance their security practices.

7. Performance issues in E-commerce

Performance issues in e-commerce can significantly impact user experience, customer satisfaction, and ultimately, business success [181]. These issues encompass various aspects, and addressing them is crucial to ensure the smooth functioning of online platforms. Performance issues in e-commerce can significantly impact user satisfaction, conversion rates, and overall business success. One of the key challenges is the load time of e-commerce websites. Slow load times can lead to increased bounce rates as impatient users are more likely to abandon a website that doesn't load quickly [182], [183]. This issue is exacerbated by the increasing use of mobile devices for online shopping, where a poor mobile experience can drive potential customers away. To address this, e-commerce platforms need to optimize website elements, leverage content delivery networks (CDNs), and invest in responsive design to ensure swift and efficient [184] loading across various devices.

Scalability is another critical performance concern, especially during peak periods such as promotions or holiday seasons. If an e-commerce platform lacks scalability, it may struggle to handle sudden increases in user traffic, leading to downtime or degraded performance [185]. Cloud-based hosting solutions that offer auto-scaling capabilities can help address this issue by dynamically adjusting resources based on demand. Additionally, regular load testing is essential to simulate high-traffic scenarios and identify potential bottlenecks in the infrastructure, allowing businesses to proactively address scalability challenges and maintain a seamless shopping experience for users even during periods of high demand.

7.1. Website Load Time

Slow website load times are a common performance challenge in e-commerce [186]. Customers expect instant access to product pages, and delays can lead to frustration and abandonment. Factors contributing to slow load times include

large images, unoptimized code, and inadequate server capacity. Implementing content delivery networks (CDNs), optimizing images, and utilizing caching mechanisms can help alleviate these issues [187].

7.2. Scalability

E-commerce platforms must be able to handle varying levels of traffic, especially during peak times such as sales events or holidays. Inadequate scalability can lead to website crashes or slowdowns [188]. Cloud-based hosting solutions, auto-scaling capabilities, and load testing are essential to ensure that the platform can handle increased demand without compromising performance.

7.3. Database Performance

Database issues, such as inefficient queries and poor indexing, can significantly impact e-commerce performance [189]. Optimizing database queries, implementing indexing strategies, and considering database sharding (dividing a database into smaller, more manageable parts) are measures that can enhance database performance and responsiveness.

7.4. Mobile Responsiveness

With the increasing use of mobile devices for online shopping, ensuring mobile responsiveness is crucial [190]. Performance issues on mobile platforms, such as slow page loading or non-optimized layouts, can lead to a poor user experience. Responsive web design, mobile-friendly images, and efficient [191] code contribute to a smoother mobile experience.

7.5. Third-Party Integrations

E-commerce platforms often integrate with third-party services, such as payment gateways, analytics tools, or marketing platforms. Performance bottlenecks can arise if these integrations are not optimized [192]. Regularly updating third-party plugins, optimizing API calls, and choosing efficient integrations help maintain a seamless user experience.

7.6. Security Measures

While security is paramount, overly stringent security measures can sometimes impact performance. Striking the right balance between robust security protocols and maintaining acceptable performance levels is crucial [193]. Implementing efficient encryption algorithms, using content security policies judiciously, and regularly updating security protocols contribute to both security and performance.

7.7. User Interface (UI) and User Experience (UX)

Cumbersome or complex user interfaces can contribute to performance issues as users navigate through the website [194]. Streamlining the UI, optimizing design elements, and employing asynchronous loading for non-essential content enhance the overall user experience and contribute to improved performance.

7.8. Monitoring and Analytics

Implementing comprehensive monitoring and analytics tools is essential for identifying and addressing performance issues promptly [195]. Continuous monitoring allows businesses to track website performance metrics, detect anomalies, and proactively optimize the platform to ensure a consistently smooth user experience.

Based on the above discussion, e-commerce businesses must adopt a holistic approach to performance optimization, addressing issues at various levels from infrastructure and coding practices to user interface design. Regular performance audits, user feedback analysis, and staying abreast of technological advancements are crucial for maintaining a competitive and high-performing e-commerce platform.

8. Future research scope in e-commerce security and privacy

The future research scope in e-commerce security and privacy is vast and critical given the evolving nature of cyber threats and the increasing reliance on online transactions. One area of focus is the exploration of innovative technologies to enhance authentication and authorization mechanisms. As traditional password-based systems remain susceptible to attacks [196], research can delve into advanced biometric authentication, adaptive access controls, and behavioral analytics to strengthen user verification processes. Additionally, the integration of artificial intelligence (AI) and machine learning (ML) algorithms [197] in anomaly detection and threat prediction can provide proactive security

measures, identifying and mitigating potential risks in real-time. Future research might also delve into the implications of emerging technologies like blockchain for securing e-commerce transactions, ensuring transparency, and building trust in online interactions.

Another crucial aspect for future research is addressing the privacy concerns associated with data collection, usage, and sharing in e-commerce. As data-driven decision-making becomes more prevalent, investigating privacy-preserving technologies such as differential privacy and homomorphic encryption is essential [198]. Research can explore methodologies to strike a balance between personalized user experiences and protecting user privacy. Moreover, with the increasing adoption of Internet of Things (IoT) devices in e-commerce, there is a need to examine the security and privacy implications of interconnected systems. Future studies can focus on developing robust frameworks and standards for securing IoT devices in the e-commerce ecosystem to prevent potential breaches and protect sensitive consumer information. Overall, the interdisciplinary nature of e-commerce security and privacy research necessitates collaboration between computer scientists, privacy experts, legal scholars, and policymakers to foster a comprehensive and adaptive approach to safeguarding online transactions and user data.

8.1. Biometric Authentication Advancements

Future research can delve into enhancing biometric authentication methods for e-commerce, exploring novel biometric identifiers and improving the accuracy and reliability of existing systems [199]-[202]. This may include the study of behavioral biometrics, such as typing patterns and mouse movements, and the development of systems resilient to spoofing attacks. Figure 11 gives an illustration of the biometric authentication process.

Biometric authentication in e-commerce enhances security by utilizing unique biological traits such as fingerprints, facial recognition, or iris scans to verify user identity. This method provides a more secure and convenient alternative to traditional passwords, reducing the risk of unauthorized access [203]. Biometric data is difficult to replicate, enhancing overall user authentication accuracy. However, it is crucial to prioritize user privacy and implement robust encryption measures to safeguard biometric information. As a result, biometric authentication contributes to a seamless and secure online shopping experience in e-commerce.

8.2. Post-Quantum Cryptography

With the potential advent of quantum computers threatening current cryptographic systems, future research can focus on post-quantum cryptography [204]. Investigating quantum-resistant algorithms and cryptographic protocols will be essential to ensure the continued security of e-commerce transactions in a quantum computing era.

8.3. Behavioral Analytics for Fraud Detection

Advancements in behavioral analytics can play a crucial role in detecting fraudulent activities in real-time [205].

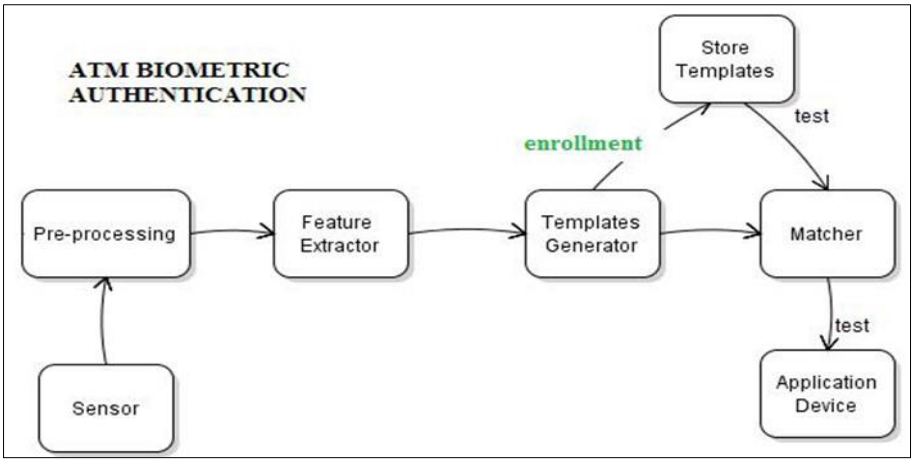

Figure 11 Biometric authentication process

Future research can explore the use of machine learning algorithms to analyze user behavior patterns, enabling the identification of anomalous activities that may indicate fraud or unauthorized access.

8.4. Privacy-Preserving Technologies

Research can delve into the development and implementation of privacy-preserving technologies such as homomorphic encryption and differential privacy [206]. These technologies allow data to be analyzed without revealing sensitive information, addressing privacy concerns associated with user data in e-commerce transactions.

8.5. Blockchain and Smart Contracts

The integration of blockchain technology in e-commerce can be a fertile area for research. Studying the use of blockchain for secure and transparent transaction processing, as well as exploring the application of smart contracts to automate and enforce privacy-preserving agreements, can be crucial. Figure 12 depicts how the blockchain technology can be incorporated into the e-commerce environment.

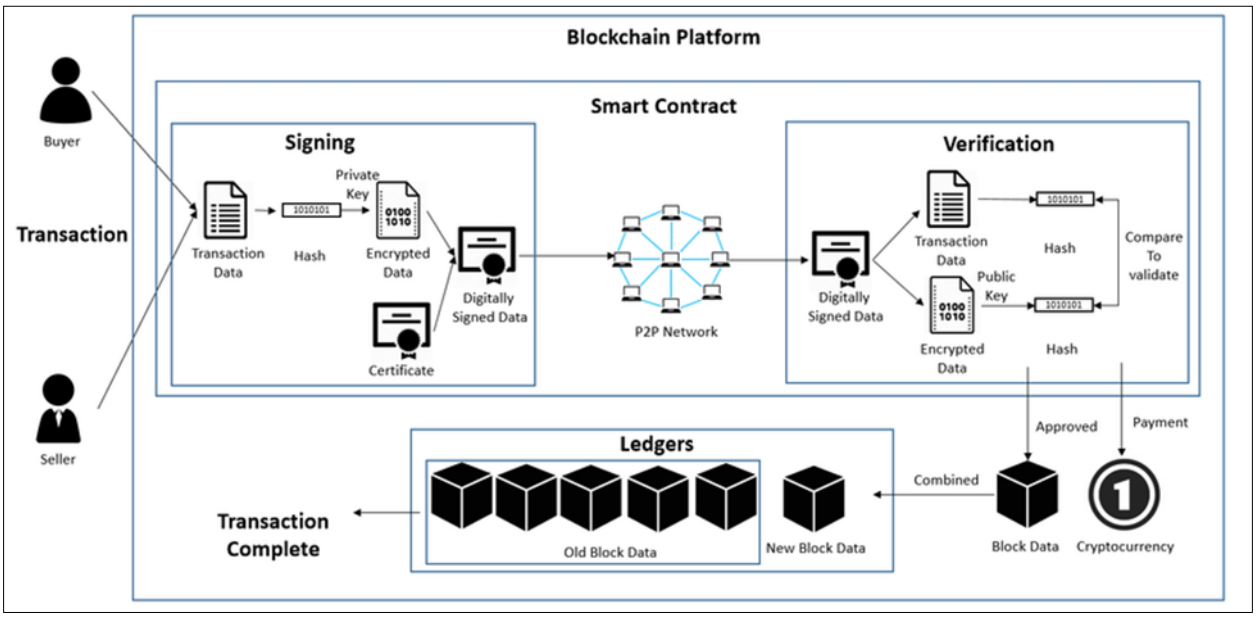

Figure 12 Blockchain in e-commerce

Blockchain technology has transformative implications for e-commerce by providing a decentralized and secure ledger that ensures transparency, immutability, and trust in transactions. In the context of e-commerce, blockchain can streamline supply chain management, reducing fraud and counterfeiting risks by offering a transparent and traceable record of product origins and movements [207], [208]. Smart contracts, self-executing agreements facilitated by blockchain, can automate various aspects of e-commerce transactions, from payment processing to order fulfillment, enhancing efficiency and minimizing the need for intermediaries. Additionally, blockchain enhances data security by decentralizing storage, mitigating the risk of data breaches. As a result, blockchain stands poised to revolutionize the e-commerce landscape, fostering increased trust among stakeholders and providing a foundation for more secure, efficient, and transparent online transactions.

8.6. IoT Security in E-commerce

As the Internet of Things (IoT) continues to grow in e-commerce, future research can focus on the security implications of interconnected devices. This includes investigating vulnerabilities, developing security standards for IoT devices, and exploring mechanisms to protect consumer privacy in the context of IoT-driven e-commerce services. Figure 13 illustrates some of the applications of IoT in e-commerce. IoT security is paramount in e-commerce as the proliferation of interconnected devices poses unique challenges [209]. Ensuring the integrity and confidentiality of data transmitted between devices, such as smart payment systems and inventory trackers, is crucial to preventing cyber threats. Implementing robust encryption protocols and regular security updates for IoT devices is essential to protect against vulnerabilities.

Employing stringent access controls and authentication mechanisms helps thwart unauthorized access to sensitive information [210]. Continuous monitoring and threat detection tools play a pivotal role in identifying and responding to potential security breaches promptly. As the e-commerce landscape increasingly relies on IoT, a comprehensive and

proactive approach to security is imperative to safeguard customer data, maintain trust, and mitigate the evolving risks associated with interconnected devices in the digital retail ecosystem.

Figure 13 IoT applications in e-commerce

8.7. Regulatory Compliance and Privacy Laws

With the evolving landscape of privacy laws globally, future research can explore the implications of these regulations on e-commerce security practices [211]. This includes studying the impact of regulations such as the GDPR (General Data Protection Regulation) and emerging laws on how e-commerce platforms handle user data.

8.8. Secure Multi-Party Computation

Research in secure multi-party computation can address privacy concerns by enabling multiple parties to jointly compute a function over their inputs while keeping those inputs private [212]. This has implications for collaborative e-commerce analytics without compromising the privacy of individual datasets.

8.9. Quantum Key Distribution (QKD)

Exploring the application of Quantum Key Distribution [213] for secure communication in e-commerce is a promising avenue. QKD leverages the principles of quantum mechanics to establish secure cryptographic keys, providing a potential solution for secure key exchange in the quantum era.

8.10. User-Centric Security Education

Future research can focus on developing effective user-centric security education approaches. Understanding user behaviors, preferences, and psychological aspects related to security can aid in designing personalized security awareness programs [214], fostering a culture of cyber hygiene among e-commerce users and reducing the likelihood of falling victim to social engineering attacks.

These research areas collectively contribute to building a more secure, private, and resilient e-commerce ecosystem, addressing the challenges posed by evolving cyber threats and technological advancements.

9. Conclusion

This paper has endeavored to illuminate the multifaceted landscape of security and privacy issues within the dynamic realm of e-commerce. As the digital marketplace becomes increasingly integral to global commerce, the imperative to fortify these platforms against cyber threats and protect user privacy has never been more pressing. The exploration of diverse challenges, including data breaches, payment gateway vulnerabilities, and phishing attacks, underscores the complexity of the security landscape in e-commerce. By recognizing these challenges, we lay the foundation for

proactive measures and informed decision-making by businesses, policymakers, and technology developers. The paper also highlights the promising avenues for addressing these challenges, including advancements in biometric authentication, post-quantum cryptography, and the integration of privacy-preserving technologies. As we venture into an era of interconnected devices and evolving regulatory landscapes, it becomes essential for stakeholders to collaborate in shaping resilient and privacy-centric e-commerce ecosystems. While acknowledging the current state of vulnerabilities, this work underscores the optimism and potential inherent in ongoing and future research endeavors aimed at securing the virtual marketplace. It is our hope that this paper contributes meaningfully to the discourse on safeguarding e-commerce platforms, ensuring the integrity of transactions, and fostering a trusted and secure online shopping experience for all stakeholders involved.

Compliance with ethical standards

Acknowledgments

Great appreciation goes to all my colleagues who supported me when I was writing this work.

References

[1] Bâra A, Oprea SV, Bucur C, Tudorică BG. Unraveling the Impact of Lockdowns on E-commerce: An Empirical Analysis of Google Analytics Data during 2019–2022. Journal of Theoretical and Applied Electronic Commerce Research. 2023 Sep 4, 18(3):1484-510.

[2] Verbivska L, Zhuk O, Ievsieieva O, Kuchmiiova T, Saienko V. The role of e-commerce in stimulating innovative business development in the conditions of european integration. Financial and credit activity-problems of theory and practice. 2023 May 1, 3(50):330-40.

[3] Antonia ID. The Influence of E-Commerce on Purchasing Decisions. JURNAL EMA. 2023 May 20, 1(2):57-66.

[4] Grewal D, Gauri DK, Roggeveen AL, Sethuraman R. Strategizing retailing in the new technology era. Journal of Retailing. 2021 Mar 1;97(1):6-12.

[5] Kedah Z. Use of e-commerce in the world of business. Startupreneur Business Digital (SABDA Journal). 2023 Feb 20, 2(1):51-60.

[6] Lucas GA, Lunardi GL, Dolci DB. From e-commerce to m-commerce: An analysis of the user's experience with different access platforms. Electronic Commerce Research and Applications. 2023 Mar 1, 58:101240.

[7] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22, 6(7):154.

[8] Gupta S, Kushwaha PS, Badhera U, Chatterjee P, Gonzalez ED. Identification of benefits, challenges, and pathways in E-commerce industries: An integrated two-phase decision-making model. Sustainable Operations and Computers. 2023 Jan 1, 4:200-18.

[9] Kumbhakar D, Sanyal K, Karforma S. An optimal and efficient data security technique through crypto-stegano for E-commerce. Multimedia Tools and Applications. 2023 Feb 8:1-4.

[10] Al-Zubaidie M, Shyaa GS. Applying Detection Leakage on Hybrid Cryptography to Secure Transaction Information in E-Commerce Apps. Future Internet. 2023 Aug 1, 15(8):262.

[11] Shyaa GS, Al-Zubaidie M. Utilizing Trusted Lightweight Ciphers to Support Electronic-Commerce Transaction Cryptography. Applied Sciences. 2023 Jun 13, 13(12):7085.

[12] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[13] Andreianu G. Protecting Your E-Commerce Business. Analysis on Cyber Security Threats. InProceedings of the International Conference on Cybersecurity and Cybercrime-2023 2023 May 30 (pp. 127-134). Asociatia Romana pentru Asigurarea Securitatii Informatiei.

[14] Prasad R. Cyber Borderlines: Exploring the Interplay Between E-Commerce and International Trade Law. Studies in Law and Justice. 2023 Oct 10, 2(4):1-9.

[15] Mohdhar A, Shaalan K. The future of e-commerce systems: 2030 and beyond. Recent Advances in Technology Acceptance Models and Theories. 2021:311-30.

[16] Khaliq Z, Khan DA, Farooq SU. Using deep learning for selenium web UI functional tests: A case-study with e-commerce applications. Engineering Applications of Artificial Intelligence. 2023 Jan 1, 117:105446.

[17] Boardman R, Chrimes C. E-commerce is King: Creating Effective Fashion Retail Website Designs. InPioneering New Perspectives in the Fashion Industry: Disruption, Diversity and Sustainable Innovation 2023 May 18 (pp. 245-254). Emerald Publishing Limited.

[18] Cai X, Cebollada J, Cortiñas M. Impact of seller-and buyer-created content on product sales in the electronic commerce platform: The role of informativeness, readability, multimedia richness, and extreme valence. Journal of Retailing and Consumer Services. 2023 Jan 1, 70:103141.

[19] Salampasis M, Katsalis A, Siomos T, Delianidi M, Tektonidis D, Christantonis K, Kaplanoglou P, Karaveli I, Bourlis C, Diamantaras K. A Flexible Session-Based Recommender System for e-Commerce. Applied Sciences. 2023 Mar 6, 13(5):3347.

[20] Ketipov R, Angelova V, Doukovska L, Schnalle R. Predicting User Behavior in e-Commerce Using Machine Learning. Cybernetics and Information Technologies. 2023 Sep 1, 23(3):89-101.

[21] Lam HY, Ho GT, Mo DY, Tang V. Responsive pick face replenishment strategy for stock allocation to fulfil e-commerce order. International Journal of Production Economics. 2023 Oct 1, 264:108976.

[22] Ji M, Liu Y, Chen X. An eye-tracking study on the role of attractiveness on consumers' purchase intentions in e-commerce live streaming. Electronic Commerce Research. 2023 Aug 10:1-36.

[23] Felix A, Rembulan GD. Analysis of Key Factors for Improved Customer Experience, Engagement, and Loyalty in the E-Commerce Industry in Indonesia. Aptisi Transactions on Technopreneurship (ATT). 2023 Sep 3, 5(2sp):196-208.

[24] Wulfert T, Woroch R, Strobel G, Seufert S, Möller F. Developing design principles to standardize e-commerce ecosystems: A systematic literature review and multi-case study of boundary resources. Electronic Markets. 2022 Dec, 32(4):1813-42.

[25] Hussain MA, Hussien ZA, Abduljabbar ZA, Ma J, Al Sibahee MA, Hussain SA, Nyangaresi VO, Jiao X. Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal. 2022 Dec 1, 23(4):145-62.

[26] Gao Q. The Application of Big Data Technology in the Efficient Development of Cross-Border E-Commerce Industry. Applied Mathematics and Nonlinear Sciences. 2023.

[27] Wang C, Zhou T, Ren M. Driving spatial network connections in rural settlements: The role of e-commerce. Applied Geography. 2023 Oct 1, 159:103067.

[28] Alazzam FA, Tubishat BM, Savchenko O, Pitel N, Diuk O. Formation of an innovative model for the development of e-commerce as part of ensuring business economic security. Business: Theory and Practice. 2023 Dec 21, 24(2):594-603.

[29] Saeed S. A customer-centric view of E-commerce security and privacy. Applied Sciences. 2023 Jan 11, 13(2):1020.

[30] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[31] Razumov P, Cherckesova L, Revyakina E, Morozov S, Medvedev D, Lobodenko A. Ensuring the security of web applications operating on the basis of the SSL/TLS protocol. InE3S Web of Conferences 2023 (Vol. 402, p. 03028). EDP Sciences.

[32] Kumar B, Roy S, Singh KU, Pandey SK, Kumar A, Sinha A, Shukla S, Shah MA, Rasool A. A Static Machine Learning Based Evaluation Method for Usability and Security Analysis in E-Commerce website. IEEE Access. 2023 Feb 22.

[33] Alqaydi L, Yeun CY, Damiani E. A Modern Solution for Identifying, Monitoring, and Selecting Configurations for SSL/TLS Deployment. InApplied Computing and Information Technology 2019 (pp. 78-88). Springer International Publishing.

[34] Zulkifli MS, Hassan NH, Maarop N, Rahim FA, Anuar MS. A Proposed Multifactor Authentication Framework for SME in Cloud Computing Environment. In2023 IEEE 13th International Conference on System Engineering and Technology (ICSET) 2023 Oct 2 (pp. 307-312). IEEE.

[35] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1, 24:100969.

[36] Gumzej R. Intelligent logistics systems in E-commerce and transportation. Mathematical Biosciences and Engineering. 2023 Jan 1, 20(2):2348-63.

[37] Ahmad AY, Gongada TN, Shrivastava G, Gabbi RS, Islam S, Nagaraju K. E-commerce trend analysis and management for Industry 5.0 using user data analysis. International Journal of Intelligent Systems and Applications in Engineering. 2023 Sep 6, 11(11s):135-50.

[38] Munshi A, Alhindi A, Qadah TM, Alqurashi A. An Electronic Commerce Big Data Analytics Architecture and Platform. Applied Sciences. 2023 Oct 4, 13(19):10962.

[39] Kalkha H, Khiat A, Bahnasse A, Ouajji H. The rising trends of smart e-commerce logistics. IEEE Access. 2023 Mar 6.

[40] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[41] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25, 4(1):10-9.

[42] Chaudhary H. Analyzing the paradigm shift of consumer behavior towards E-Commerce during pandemic lockdown. Available at SSRN 3664668. 2020 Jul 31.

[43] Sikder AS, Rolfe S. The Power of E-Commerce in the Global Trade Industry: A Realistic Approach to Expedite Virtual Market Place and Online Shopping from anywhere in the World.: E-Commerce in the Global Trade Industry. International Journal of Imminent Science & Technology. 2023, 1(1):79-100.

[44] Semerádová T, Weinlich P. The Broad and Narrow Definition of E-Commerce. InAchieving Business Competitiveness in a Digital Environment: Opportunities in E-commerce and Online Marketing 2022 Jan 22 (pp. 1-26). Cham: Springer International Publishing.

[45] Tokar T, Jensen R, Williams BD. A guide to the seen costs and unseen benefits of e-commerce. Business Horizons. 2021 May 1, 64(3):323-32.

[46] Fedushko S, Ustyianovych T. E-commerce customers behavior research using cohort analysis: A case study of COVID-19. Journal of Open Innovation: Technology, Market, and Complexity. 2022 Jan 6, 8(1):12.

[47] Silitonga D, Rohmayanti SA, Aripin Z, Kuswandi D, Sulistyo AB. Edge Computing in E-commerce Business: Economic Impacts and Advantages of Scalable Information Systems. EAI Endorsed Transactions on Scalable Information Systems. 2024, 11(1).

[48] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[49] Allioui H, Mourdi Y. Unleashing the potential of AI: Investigating cutting-edge technologies that are transforming businesses. International Journal of Computer Engineering and Data Science (IJCEDS). 2023 Aug 16, 3(2):1-2.

[50] Fan Z, Wang Y, Ying Z. Empowerment of Cross-Border E-Commerce Platforms for Small and Medium-Sized Enterprises: Evidence from China. Journal of Business-to-Business Marketing. 2023 Jan 2, 30(1):33-44.

[51] Bubanja I, Vidas BM. Managing trade transactions in the covid era: The rise of e-commerce. Journal of Engineering Management and Competitiveness (JEMC). 2022, 12(1):20-34.

[52] Sutrisno S, Kuraesin AD, Siminto S, Irawansyah I, Ausat AM. The Role of Information Technology in Driving Innovation and Entrepreneurial Business Growth. Jurnal Minfo Polgan. 2023 May 27, 12(2):586-97.

[53] Daraojimba C, Abioye KM, Bakare AD, Mhlongo NZ, Onunka O, Daraojimba DO. Technology and Innovation to Growth of Entrepreneurship and Financial Boost: A Decade in Review (2013-2023). International Journal of Management & Entrepreneurship Research. 2023 Nov 2, 5(10):769-92.

[54] Yenurkar GK, Mal S, Nyangaresi VO, Hedau A, Hatwar P, Rajurkar S, Khobragade J. Multifactor data analysis to forecast an individual's severity over novel COVID-19 pandemic using extreme gradient boosting and random forest classifier algorithms. Engineering Reports. 2023:e12678.

[55] Costa P, Rodrigues H. The ever-changing business of e-commerce-net benefits while designing a new platform for small companies. Review of Managerial Science. 2023 Jul 20:1-39.

[56] Taher G. E-commerce: advantages and limitations. International Journal of Academic Research in Accounting Finance and Management Sciences. 2021 Jan, 11(1):153-65.

[57] Rao P, Balasubramanian S, Vihari N, Jabeen S, Shukla V, Chanchaichujit J. The e-commerce supply chain and environmental sustainability: An empirical investigation on the online retail sector. Cogent Business & Management. 2021 Jan 1, 8(1):1938377.

[58] Youssef HA, Hossam AT. Privacy Issues in AI and Cloud Computing in E-commerce Setting: A Review. International Journal of Responsible Artificial Intelligence. 2023 Jul 16, 13(7):37-46.

[59] Srivastava S, Jeet S. E-commerce and privacy issues. Russian Law Journal. 2023, 11(5):2170-5.

[60] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[61] Tao S, Liu Y, Sun C. Understanding information sensitivity perceptions and its impact on information privacy concerns in e-commerce services: Insights from China. Computers & Security. 2023 Dec 12:103646.

[62] Liu R, Wang E. Blockchain and mobile client privacy protection in e-commerce consumer shopping tendency identification application. Soft Computing. 2023 May, 27(9):6019-31.

[63] Gatziolis KG, Tselikas ND, Moscholios ID. Adaptive user profiling in E-commerce and administration of public services. Future Internet. 2022 May 9, 14(5):144.

[64] Ermolaev E, Abellán Álvarez I, Sedlmeir J, Fridgen G. z-Commerce: Designing a Data-Minimizing One-Click Checkout Solution. InInternational Conference on Design Science Research in Information Systems and Technology 2023 May 19 (pp. 3-17). Cham: Springer Nature Switzerland.

[65] Zhu K. Blockchain Technology: Applications, Opportunities, Challenges, and Countermeasures. In2023 International Conference on Finance, Trade and Business Management (FTBM 2023) 2023 Nov 30 (pp. 460-468). Atlantis Press.

[66] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[67] Mao R, Chen H, Shen H. Cooperation strategies with third-party platform: E-tailer and manufacturer perspectives. Naval Research Logistics (NRL). 2023 Dec, 70(8):878-96.

[68] He B, Mirchandani P, Yang G. Offering custom products using a C2M model: Collaborating with an E-commerce platform. International Journal of Production Economics. 2023 Aug 1, 262:108918.

[69] Ali SA. desigining secure and robust e-commerce plaform for public cloud. The Asian Bulletin of Big Data Management. 2023 Nov 25, 3(1).

[70] Ge X. Analysis of legal framework solutions to protect retail consumers. International Journal of Retail & Distribution Management. 2023 May 18.

[71] Ahi AA, Sinkovics N, Sinkovics RR. E-commerce policy and the global economy: A path to more inclusive development?. Management International Review. 2023 Feb, 63(1):27-56.

[72] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28, 15(13):10264.

[73] Heikkilä E, Tiusanen R, Öz E. Towards requirements for third-party assessments in the Specific Operations Risk Assessment process. In2023 International Conference on Unmanned Aircraft Systems (ICUAS) 2023 Jun 6 (pp. 207-212). IEEE.

[74] Bandari V. Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types. International Journal of Business Intelligence and Big Data Analytics. 2023 Jan 20, 6(1):1-1.

[75] Strycharz J, van Noort G, Helberger N, Smit E. Contrasting perspectives–practitioner's viewpoint on personalised marketing communication. European Journal of Marketing. 2019 Apr 30, 53(4):635-60.

[76] Tseng HT, Nadeem W, Hajli MS, Featherman M, Hajli N. Understanding consumers' interest in social commerce: the role of privacy, trust and security. Information Technology & People. 2023 Nov 7.

[77] Kaili M, Kapitsaki GM. Improving the Representation Choices of Privacy Policies for End-Users. InInternational Conference on Web Information Systems and Technologies 2022 Oct 25 (pp. 42-59). Cham: Springer Nature Switzerland.

[78] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[79] Fakhouri HN, Alawadi S, Awaysheh FM, Hamad F, Alzubi S, AlAdwan MN. An Overview of using of Artificial Intelligence in Enhancing Security and Privacy in Mobile Social Networks. In2023 Eighth International Conference on Fog and Mobile Edge Computing (FMEC) 2023 Sep 18 (pp. 42-51). IEEE.

[80] Gupta K, Mane P, Rajankar OS, Bhowmik M, Jadhav R, Yadav S, Rawandale S, Chobe SV. Harnessing AI for Strategic Decision-Making and Business Performance Optimization. International Journal of Intelligent Systems and Applications in Engineering. 2023 Aug 16, 11(10s):893-912.

[81] Gavrilova ML, Anzum F, Hossain Bari AS, Bhatia Y, Iffath F, Ohi Q, Shopon M, Wahid Z. A multifaceted role of biometrics in online security, privacy, and trustworthy decision making. InBreakthroughs in Digital Biometrics and Forensics 2022 Oct 15 (pp. 303-324). Cham: Springer International Publishing.

[82] Xiao Y, Zhou C, Guo X, Song Y, Chen C. A Novel Decentralized E-Commerce Transaction System Based on Blockchain. Applied Sciences. 2022 Jun 7, 12(12):5770.

[83] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31, 47(6).

[84] Weber PA, Zhang N, Wu H. A comparative analysis of personal data protection regulations between the EU and China. Electronic Commerce Research. 2020 Sep, 20:565-87.

[85] Martínez-Martínez DF. Unification of personal data protection in the European Union: Challenges and implications. Profesional de la Informacion. 2018 Feb 12, 27(1):185-94.

[86] Gijrath S, Zwenne GJ, Lodder AR, Hof SV. Concise european data protection, e-commerce and IT law. Concise European Data Protection, E-Commerce and IT Law. 2018:1-058.

[87] Hassan A, Ahmed K. Cybersecurity's Impact on Customer Experience: An Analysis of Data Breaches and Trust Erosion. Emerging Trends in Machine Intelligence and Big Data. 2023 Sep 23, 15(9):1-9.

[88] Aldboush HH, Ferdous M. Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust. International Journal of Financial Studies. 2023 Jul 10, 11(3):90.

[89] Nyangaresi VO, Yenurkar GK. Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor networks. High-Confidence Computing. 2023 Nov 24:100178.

[90] Kumar I. Emerging Threats in Cybersecurity: A Review Article. International Journal of Applied and Natural Sciences. 2023 Jul 13, 1(1):01-8.

[91] Santos V, Augusto T, Vieira J, Bacalhau L, Sousa BM, Pontes D. E-Commerce: Issues, Opportunities, Challenges, and Trends. Promoting Organizational Performance Through 5G and Agile Marketing. 2023:224-44.

[92] Sankar JG, David A, Valan P. Examining User Understanding and Perceptions of E-Commerce Data Privacy, Security, and Protection. InConfronting Security and Privacy Challenges in Digital Marketing 2023 (pp. 159-185). IGI Global.

[93] Bajracharya S, Chatterjee JM. Challenges for online purchase intention: a qualitative study of e-commerce sector of Nepal. LBEF Res. J. Sci. Technol. Manage.. 2023, 5:21-33.

[94] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11, 10:26257-70.

[95] D'Adamo I, González-Sánchez R, Medina-Salgado MS, Settembre-Blundo D. E-commerce calls for cyber-security and sustainability: How european citizens look for a trusted online environment. Sustainability. 2021 Jun 15, 13(12):6752.

[96] Zhu B, Ahamat H. The Role of E-commerce Adoption in Enhancing Regulatory Compliance in Information Systems of Foreign Investment Management in Malaysia-A Moderating Effect of Innovation Management. Journal of Information Systems Engineering and Management. 2023, 8(3):21797.

[97] Štitilis D, Laurinaitis M, Verenius E. The Use of biometric technologies in ensuring critical infrastructure security: the context of protecting personal data. Entrepreneurship and sustainability issues. 2023, 10:133-50.

[98] Utegen D, Rakhmetov BZ. Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models. Journal of Digital Technologies and Law. 2023, 1(3):825-44.

[99] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[100] Abu-ulbeh W, Al Moaiad Y, Liban A, Farea MM, Al-Haithami WA, El-Ebiary YA. The Threats and Dimensions of Security Systems in Electronic Commerce. Journal of Survey in Fisheries Sciences. 2023 Apr 3, 10(2S):2667-83.

[101] Senapati KK, Kumar A, Sinha K. Impact of Information Leakage and Conserving Digital Privacy. InMalware Analysis and Intrusion Detection in Cyber-Physical Systems 2023 (pp. 166-188). IGI Global.

[102] Singh Y, Sinha S. Challenges and solutions for e-commerce application. Journal of Data Acquisition and Processing. 2023, 38(3):1898.

[103] Madyatmadja ED, Karsen M, Yuri A, Sijabat DP, Rhaka G, Santika R, Pristinella D. The effectiveness of security and customer convenience in the use of e-commerce. Journal of System and Management Sciences. 2023, 13(3):193-204.

[104] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[105] Omotunde H, Ahmed M. A comprehensive review of security measures in database systems: Assessing authentication access control and beyond. Mesopotamian J. Cyber Secur.. 2023 Aug, 2023:115-33.

[106] James E, Rabbi F. Fortifying the IoT Landscape: Strategies to Counter Security Risks in Connected Systems. Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries. 2023 Jan 9, 6(1):32-46.

[107] Muhammad T, Munir MT, Munir MZ, Zafar MW. Integrative Cybersecurity: Merging Zero Trust, Layered Defense, and Global Standards for a Resilient Digital Future. International journal of computer science and technology. 2022 Nov 30, 6(4):99-135.

[108] Colomb Y, White P, Islam R, Alsadoon A. Applying Zero Trust Architecture and Probability-Based Authentication to Preserve Security and Privacy of Data in the Cloud. InEmerging Trends in Cybersecurity Applications 2022 Nov 19 (pp. 137-169). Cham: Springer International Publishing.

[109] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[110] Beju DG, Făt CM. Frauds in Banking System: Frauds with Cards and Their Associated Services. InEconomic and Financial Crime, Sustainability and Good Governance 2023 Aug 27 (pp. 31-52). Cham: Springer International Publishing.

[111] Hari Teja AS, Lavaraju B. An Empirical Study on Credit Card Fraud in Legal Approach. Legal Lock J.. 2023, 2:10.

[112] Nagre A, Sen A. Study Of Security Postures In Payment Gateways Using a Case Study Approach. In2022 International Conference on Decision Aid Sciences and Applications (DASA) 2022 Mar 23 (pp. 534-538). IEEE.

[113] Bradford T. The Puzzle of Payments Security: Fitting the Pieces Together to Protect the Retail Payments System. Payments System Research Briefing. 2015 Oct(Oct.):1-5.

[114] Saini J. Security Protocol of Social Payment Apps. InIntelligent, Secure, and Dependable Systems in Distributed and Cloud Environments: First International Conference, ISDDC 2017, Vancouver, BC, Canada, October 26-28, 2017, Proceedings 1 2017 (pp. 139-150). Springer International Publishing.

[115] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014, 16(5):137-44.

[116] Varshney G, Kumawat R, Varadharajan V, Tupakula U, Gupta C. Anti-phishing: A comprehensive perspective. Expert Systems with Applications. 2024 Mar 15, 238:122199.

[117] Carroll F, Adejobi JA, Montasari R. How good are we at detecting a phishing attack? investigating the evolving phishing attack email and why it continues to successfully deceive society. SN Computer Science. 2022 Mar, 3(2):170.

[118] Permana FA, Jamaludin A. Personal Data Vulnerability in the Digital Era: Study of Modus Operandi and Mechanisms to Prevent Phishing Crimes. Jurnal Al-Hakim: Jurnal Ilmiah Mahasiswa, Studi Syariah, Hukum dan Filantropi. 2023 Nov 21:201-16.

[119] Akartuna EA, Johnson SD, Thornton AE. The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review. Security Journal. 2023 Dec, 36(4):615-50.

[120] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1, 133:102763.

[121] Alshamrani A, Myneni S, Chowdhary A, Huang D. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials. 2019 Jan 9, 21(2):1851-77.

[122] Abbas SG, Vaccari I, Hussain F, Zahid S, Fayyaz UU, Shah GA, Bakhshi T, Cambiaso E. Identifying and mitigating phishing attack threats in IoT use cases using a threat modelling approach. Sensors. 2021 Jul 14, 21(14):4816.

[123] de Neira AB, Kantarci B, Nogueira M. Distributed denial of service attack prediction: Challenges, open issues and opportunities. Computer Networks. 2023 Feb 1, 222:109553.

[124] Shah Z, Ullah I, Li H, Levula A, Khurshid K. Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. Sensors. 2022 Jan 31, 22(3):1094.

[125] Fathima A, Devi GS, Faizaanuddin M. Improving distributed denial of service attack detection using supervised machine learning. Measurement: Sensors. 2023 Dec 1, 30:100911.

[126] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[127] Aldhyani TH, Alkahtani H. Artificial Intelligence Algorithm-Based Economic Denial of Sustainability Attack Detection Systems: Cloud Computing Environments. Sensors. 2022 Jun 21, 22(13):4685.

[128] Shukla P, Krishna CR, Patil NV. Iot traffic-based DDoS attacks detection mechanisms: A comprehensive review. The Journal of Supercomputing. 2023 Dec 19:1-58.

[129] Tikhe GN, Patheja PS. Mitigation of Distributed Denial of Service (DDoS) Attack Using Network Function Virtualization. InSecurity, Privacy and Data Analytics: Select Proceedings of the 2nd International Conference, ISPDA 2022 2023 Sep 19 (Vol. 1049, p. 311). Springer Nature.

[130] Kumari P, Jain AK. A comprehensive study of DDoS attacks over IoT network and their countermeasures. Computers & Security. 2023 Jan 13:103096.

[131] Ennafiri M, Charaf ME, Abdessalam AI. Towards Secure Transactions with IoT: An Advanced Smart Payment Solution. In2023 3rd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET) 2023 May 18 (pp. 01-06). IEEE.

[132] Nyangaresi VO, Abd-Elnaby M, Eid MM, Nabih Zaki Rashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 Sep, 33(9):e4528.

[133] Bojjagani S, Sastry VN, Chen CM, Kumari S, Khan MK. Systematic survey of mobile payments, protocols, and security infrastructure. Journal of Ambient Intelligence and Humanized Computing. 2023 Jan, 14(1):609-54.

[134] Al-Okaily M, Rahman MS, Ali A, Abu-Shanab E, Masa'deh RE. An empirical investigation on acceptance of mobile payment system services in Jordan: extending UTAUT2 model with security and privacy. International Journal of Business Information Systems. 2023, 42(1):123-52.

[135] Wang F, Yang N, Shakeel PM, Saravanan V. Machine learning for mobile network payment security evaluation system. Transactions on Emerging Telecommunications Technologies. 2021 Jan 28:e4226.

[136] Khalek SA, Behera CK, Samanta T. An integrated framework for understanding information disclosure behaviour in mobile payment services. Journal of Financial Services Marketing. 2023 Oct 26:1-22.

[137] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19, 11(3):55.

[138] Taherdoost H. E-Business Security and Control. InE-Business Essentials: Building a Successful Online Enterprise 2023 Sep 5 (pp. 105-135). Cham: Springer Nature Switzerland.

[139] Mahmud SY, English KV, Thorn S, Enck W, Oest A, Saad M. Analysis of Payment Service Provider SDKs in Android. InProceedings of the 38th Annual Computer Security Applications Conference 2022 Dec 5 (pp. 576-590).

[140] Khan A, Ahmad A, Ahmed M, Sessa J, Anisetti M. Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends. Complex & Intelligent Systems. 2022 Oct, 8(5):3919-41.

[141] Singh I, Singh B. Access management of IoT devices using access control mechanism and decentralized authentication: A review. Measurement: Sensors. 2023 Feb 1, 25:100591.

[142] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023 Mar 11, 12(6):1333.

[143] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[144] Zhang R, Fang L, He X, Wei C. Controlling Information Risk in E-commerce. InThe Whole Process of E-commerce Security Management System: Design and Implementation 2023 Feb 4 (pp. 61-120). Singapore: Springer Nature Singapore.

[145] Zhang R, Fang L, He X, Wei C. Controlling Transaction Risk in E-commerce. InThe Whole Process of E-commerce Security Management System: Design and Implementation 2023 Feb 4 (pp. 181-224). Singapore: Springer Nature Singapore.

[146] Dahal SB. Enhancing E-commerce Security: The Effectiveness of Blockchain Technology in Protecting Against Fraudulent Transactions. International Journal of Information and Cybersecurity. 2023 Feb 20, 7(1):1-2.

[147] Shen H, Wu G, Xia Z, Susilo W, Zhang M. A Privacy-Preserving and Verifiable Statistical Analysis Scheme for an E-Commerce Platform. IEEE Transactions on Information Forensics and Security. 2023 Apr 24.

[148] Yasmeen G, Afaq SA. The critical analysis of E-Commerce web application vulnerabilities. InAdvances in Cyberology and the Advent of the Next-Gen Information Revolution 2023 (pp. 22-37). IGI Global.

[149] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan, 13(2):691.

[150] Pourrahmani H, Yavarinasab A, Monazzah AM, Van Herle J. A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain. Internet of Things. 2023 Aug 5:100888.

[151] Wu X, Du Y, Fan T, Guo J, Ren J, Wu R, Zheng T. Threat analysis for space information network based on network security attributes: a review. Complex & Intelligent Systems. 2023 Jun, 9(3):3429-68.

[152] Arogundade OR. Network Security Concepts, Dangers, and Defense Best Practical. Computer Engineering and Intelligent Systems. 2023, 14(2).

[153] Gola KK, Arya S, Khan G, Devkar C, Chaurasia N. Security analysis of fog computing environment for ensuring the security and privacy of information. Transactions on Emerging Telecommunications Technologies. 2023 Oct, 34(10):e4861.

[154] Jaime FJ, Muñoz A, Rodríguez-Gómez F, Jerez-Calero A. Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare. Sensors. 2023 Nov 3, 23(21):8944.

[155] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[156] Agarwal M. An Empirical Study of E-Commerce Security, Challenges and their Solutions. european journal of innovation in nonformal education. 2023 Jul 23, 3(7):150-63.

[157] Gutfleisch M, Schöps M, Horstmann SA, Wichmann D, Sasse MA. Security Champions Without Support: Results from a Case Study with OWASP SAMM in a Large-Scale E-Commerce Enterprise. InProceedings of the 2023 European Symposium on Usable Security 2023 Oct 16 (pp. 260-276).

[158] Khan WZ, Rafique W, Haider N, Hakak S, Imran M. Internet of Everything: Enabling Technologies, Applications, Security and Challenges. Authorea Preprints. 2023 Oct 30.

[159] Badawy W. Data-driven framework for evaluating digitization and artificial intelligence risk: a comprehensive analysis. AI and Ethics. 2023 Nov 20:1-26.

[160] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1, 11(1):185-94.

[161] Altayaran S, Elmedany W. Security threats of application programming interface (API's) in internet of things (IoT) communications. In4th Smart Cities Symposium (SCS 2021) 2021 Nov 21 (Vol. 2021, pp. 552-557). IET.

[162] Girma A, Guo MA, Irungu J. Identifying Shared Security Vulnerabilities and Mitigation Strategies at the Intersection of Application Programming Interfaces (APIs), Application-Level and Operating System (OS) of Mobile Devices. InProceedings of the Future Technologies Conference 2022 Oct 13 (pp. 499-513). Cham: Springer International Publishing.

[163] Idris M, Syarif I, Winarno I. Development of vulnerable web application based on owasp api security risks. In2021 International Electronics Symposium (IES) 2021 Sep 29 (pp. 190-194). IEEE.

[164] Meng N, Nagy S, Yao D, Zhuang W, Argoty GA. Secure coding practices in java: Challenges and vulnerabilities. InProceedings of the 40th International Conference on Software Engineering 2018 May 27 (pp. 372-383).

[165] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1, 142:103117.

[166] Engert M, Evers J, Hein A, Krcmar H. The engagement of complementors and the role of platform boundary resources in e-commerce platform ecosystems. Information Systems Frontiers. 2022 Dec, 24(6):2007-25.

[167] Shreyas S. Security Model for Cloud Computing: Case Report of Organizational Vulnerability. Journal of Information Security. 2023 Aug 8, 14(4):250-63.

[168] Ahmad H, Dharmadasa I, Ullah F, Babar MA. A review on c3i systems' security: Vulnerabilities, attacks, and countermeasures. ACM Computing Surveys. 2023 Jan 13, 55(9):1-38.

[169] Nankya M, Chataut R, Akl R. Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies. Sensors. 2023 Oct 30, 23(21):8840.

[170] Varadharajan V, Tupakula U, Karmakar KK. Techniques for Enhancing Security in Industrial Control Systems. ACM Transactions on Cyber-Physical Systems. 2023.

[171] Javaid M, Haleem A, Singh RP, Suman R. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications. 2023 Mar 11:100016.

[172] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[173] Tian YC, Gao J. Network Security and Privacy Architecture. InNetwork Analysis and Architecture 2023 Oct 1 (pp. 361-402). Singapore: Springer Nature Singapore.

[174] Khan MJ. Securing network infrastructure with cyber security. World Journal of Advanced Research and Reviews. 2023, 17(2):803-13.

[175] Biswakarma G, Bhusal P. Banks' Level Factors Affecting the Effective Implementation of Anti-Money Laundering Practices in Nepalese Banks: An Employee and Customer Perspectives. South Asian Journal of Finance. 2023, 3(1):1-22.

[176] Thomas G, Sule MJ. A service lens on cybersecurity continuity and management for organizations' subsistence and growth. Organizational Cybersecurity Journal: Practice, Process and People. 2023 Sep 18, 3(1):18-40.

[177] Saeed S, Altamimi SA, Alkayyal NA, Alshehri E, Alabbad DA. Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors. 2023 Jul 25, 23(15):6666.

[178] Nyangaresi VO, Ogundoyin SO. Certificate based authentication scheme for smart homes. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[179] Stewart H. Digital transformation security challenges. Journal of Computer Information Systems. 2023 Jul 4, 63(4):919-36.

[180] Chauhan M, Shiaeles S. An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. Network. 2023 Sep 12, 3(3):422-50.

[181] Mamakou XJ, Zaharias P, Milesi M. Measuring customer satisfaction in electronic commerce: The impact of e-service quality and user experience. International Journal of Quality & Reliability Management. 2023 Sep 14.

[182] Tam C, Loureiro A, Oliveira T. The individual performance outcome behind e-commerce: Integrating information systems success and overall trust. Internet Research. 2020 Apr 6, 30(2):439-62.

[183] Costa P, Rodrigues H. The ever-changing business of e-commerce-net benefits while designing a new platform for small companies. Review of Managerial Science. 2023 Jul 20:1-39.

[184] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[185] Muhammad T. A Comprehensive Study on Software-Defined Load Balancers: Architectural Flexibility & Application Service Delivery in On-Premises Ecosystems. International Journal Of Computer Science And Technology. 2022 Mar 31, 6(1):1-24.

[186] Tuncer R, Sergeeva A, Bongard-Blanchy K, Distler V, Doublet S, Koenig V. Running out of time (rs): effects of scarcity cues on perceived task load, perceived benevolence and user experience on e-commerce sites. Behaviour & Information Technology. 2023 Aug 3:1-9.

[187] Zolfaghari B, Srivastava G, Roy S, Nemati HR, Afghah F, Koshiba T, Razi A, Bibak K, Mitra P, Rai BK. Content delivery networks: State of the art, trends, and future roadmap. ACM Computing Surveys (CSUR). 2020 Apr 16, 53(2):1-34.

[188] Chellam VV, Praveenkumar S, Kumar B, Rajput N, Yagnam N, Rajak PK, Dalal T. E-Commerce Business Modeling in Smart Cities. InHandbook of Research on Data-Driven Mathematical Modeling in Smart Cities 2023 (pp. 192-223). IGI Global.

[189] Malhotra D, Rishi O. An intelligent approach to design of E-Commerce metasearch and ranking system using next-generation big data analytics. Journal of King Saud University-Computer and Information Sciences. 2021 Feb 1, 33(2):183-94.

[190] Alalwan AA, Algharabat RS, Baabdullah AM, Rana NP, Qasem Z, Dwivedi YK. Examining the impact of mobile interactivity on customer engagement in the context of mobile shopping. Journal of Enterprise Information Management. 2020 Apr 22, 33(3):627-53.

[191] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[192] Wu M, Liu Y, Chung HF, Guo S. When and how mobile payment platform complementors matter in cross-border B2B e-commerce ecosystems? An integration of process and modularization analysis. Journal of Business Research. 2022 Feb 1, 139:843-54.

[193] Shen S, Zhu T, Wu D, Wang W, Zhou W. From distributed machine learning to federated learning: In the view of data privacy and security. Concurrency and Computation: Practice and Experience. 2022 Jul 25, 34(16):e6002.

[194] Abascal J, Arrue M, Valencia X. Tools for web accessibility evaluation. Web accessibility: a foundation for research. 2019:479-503.

[195] Sheikh RA, Bhatia S, Metre SG, Faqihi AY. Strategic value realization framework from learning analytics: a practical approach. Journal of Applied Research in Higher Education. 2022 Mar 14, 14(2):693-713.

[196] Amador J, Ma Y, Hasama S, Lumba E, Lee G, Birrell E. Prospects for improving password selection. InNineteenth Symposium on Usable Privacy and Security (SOUPS 2023) 2023 (pp. 263-282).

[197] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec, 39(10):e13126.

[198] Kumar GS, Premalatha K, Maheshwari GU, Kanna PR. No more privacy Concern: A privacy-chain based homomorphic encryption scheme and statistical method for privacy preservation of user's private and sensitive data. Expert Systems with Applications. 2023 Dec 30, 234:121071.

[199] Alabi S, White M, Beloff N. Contactless palm vein authentication security technique for better adoption of e-commerce in developing countries. InIntelligent Computing: Proceedings of the 2020 Computing Conference, Volume 3 2020 (pp. 380-390). Springer International Publishing.

[200] Liébana-Cabanillas F, Kalinic Z, Muñoz-Leiva F, Higueras-Castillo E. Biometric m-payment systems: A multi-analytical approach to determining use intention. Information & Management. 2023 Dec 17:103907.

[201] Krennhuber S, Stabauer M. E-Commerce and Covid-19: An Analysis of Payment Transactions and Consumer Preferences. InInternational Conference on Human-Computer Interaction 2023 Jul 17 (pp. 219-229). Cham: Springer Nature Switzerland.

[202] Harika D, Noorullah S. Implementation of image authentication using digital watermarking with biometric. International Journal of Engineering Technology and Management Sciences. 2023, 7(1):154-67.

[203] Al Sibahee MA, Nyangaresi VO, Abduljabbar ZA, Luo C, Zhang J, Ma J. Two-Factor Privacy Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks. IEEE Internet of Things Journal. 2023 Dec 7.

[204] Sharma P, Gupta V, Sood SK. Post-Quantum Cryptography Research Landscape: A Scientometric Perspective. Journal of Computer Information Systems. 2023 Sep 27:1-22.

[205] Patel K. Credit Card Analytics: A Review of Fraud Detection and Risk Assessment Techniques. International Journal of Computer Trends and Technology. 2023, 71(10):69-79.

[206] Jia B, Zhang X, Liu J, Zhang Y, Huang K, Liang Y. Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT. IEEE Transactions on Industrial Informatics. 2021 Jun 8, 18(6):4049-58.

[207] Jebamikyous H, Li M, Suhas Y, Kashef R. Leveraging machine learning and blockchain in E-commerce and beyond: benefits, models, and application. Discover Artificial Intelligence. 2023 Jan 10, 3(1):3.

[208] Sekar S, Solayappan A, Srimathi J, Raja S, Durga S, Manoharan P, Hamdi M, Tunze GB. Autonomous transaction model for e-commerce management using blockchain technology. International Journal of Information Technology and Web Engineering (IJITWE). 2022 Jan 1, 17(1):1-4.

[209] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[210] Khan I, Ghani A, Saqlain SM, Ashraf MU, Alzahrani A, Kim DH. Secure Medical Data Against Unauthorized Access using Decoy Technology in Distributed Edge Computing Networks. IEEE Access. 2023 Dec 18.

[211] Chawla N, Kumar B. E-commerce and consumer protection in India: the emerging trend. Journal of Business Ethics. 2022 Oct, 180(2):581-604.

[212] Zhou J, Feng Y, Wang Z, Guo D. Using secure multi-party computation to protect privacy on a permissioned blockchain. Sensors. 2021 Feb 23, 21(4):1540.

[213] Mehic M, Niemiec M, Rass S, Ma J, Peev M, Aguado A, Martin V, Schauer S, Poppe A, Pacher C, Voznak M. Quantum key distribution: a networking perspective. ACM Computing Surveys (CSUR). 2020 Sep 28, 53(5):1-41.

[214] Chaudhary S, Gkioulos V, Katsikas S. A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Computer Science Review. 2023 Nov 1, 50:100592.