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

Data protection and privacy in e-commerce environment: Systematic review

Elizabeth Atieno Otieno *

Jaramogi Oginga Odinga University of Science and Technology, 40601, Bondo.

GSC Advanced Research and Reviews, 2025, 22(01), 238-271

Publication history: Received on 10 December 2024; revised on 18 January 2025; accepted on 21 January 2025

Article DOI: https://doi.org/10.30574/gscarr.2025.22.1.0024

Abstract

The rapid expansion of e-commerce has revolutionized how businesses and consumers interact, but it has also raised significant concerns regarding data protection and privacy. This systematic review examines existing research on data protection and privacy in the e-commerce environment, with a focus on identifying key challenges, solutions, and trends. A comprehensive search of academic databases was conducted, covering studies published over the last two decades. The findings highlight the vulnerabilities inherent in e-commerce systems, including data breaches, identity theft, and inadequate compliance with evolving privacy regulations such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). Emerging technologies such as blockchain, artificial intelligence, and privacy-preserving algorithms are explored as potential solutions to enhance data security and consumer trust. Additionally, the review underscores the critical role of user awareness, organizational practices, and regulatory enforcement in creating a robust data protection framework. This paper aims to provide researchers, policymakers, and industry stakeholders with a consolidated understanding of current practices and future directions for safeguarding data privacy in the e-commerce sector.

Keywords: E-commerce; Data protection; Privacy; Security; Performance.

1. Introduction

The rapid growth of e-commerce has revolutionized the way businesses and consumers interact, leading to the digitalization of global trade and the establishment of virtual marketplaces [1]-[3]. Online shopping has become an essential part of modern commerce, offering consumers the convenience of purchasing goods and services from anywhere in the world. Figure 1 gives a depiction of a typical e-commerce workflow. According to the latest global statistics, e-commerce has seen exponential growth, with the global retail e-commerce sales expected to surpass $7 trillion by 2025. However, this tremendous growth in e-commerce transactions has brought with it a host of challenges, particularly concerning data protection and privacy [4]-[6]. As businesses collect vast amounts of personal, financial, and behavioral data from users, the risks of data breaches, identity theft, fraud, and privacy violations have become a critical concern for both consumers and e-commerce platforms alike [7], [8].

* Corresponding author: Elizabeth Atieno Otieno

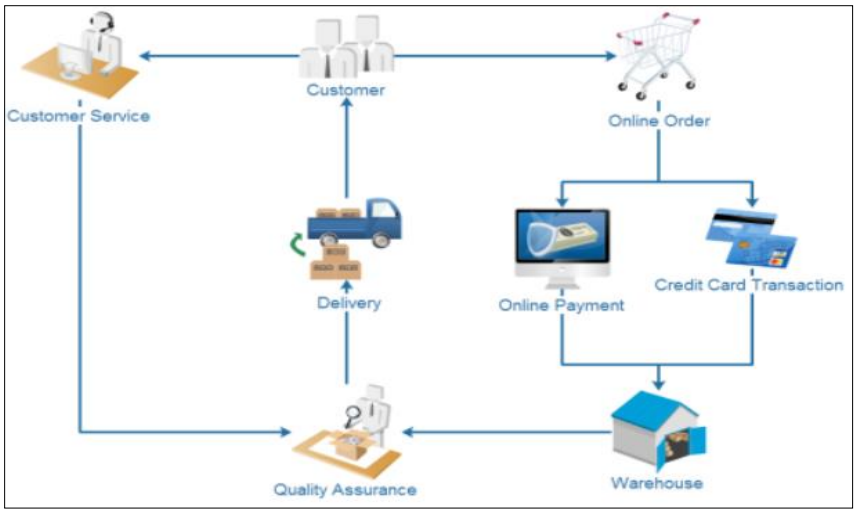

Figure 1 E-commerce workflow

Data protection and privacy have emerged as two of the most pressing issues in the digital economy, especially within the e-commerce sector [9]. Personal information, including credit card details, shipping addresses, and purchase history, is continuously exchanged and stored by e-commerce platforms [10]. This makes e-commerce platforms prime targets for cyberattacks, such as data breaches and ransomware, which often result in the exposure of sensitive data [11], [12]. Figure 2 shows some of the most common threats in e-commerce.

Figure 2 Common threats in e-commerce

Moreover, the growing concern over how personal data is collected, shared, and utilized by businesses has intensified the demand for stronger privacy protections [13]. In response, various data protection frameworks, such as the GDPR in the European Union and the CCPA in the United States, have been introduced to protect consumers' privacy rights and ensure compliance among businesses. However, ensuring compliance with these regulations, while maintaining efficient operations, has posed significant challenges for e-commerce businesses.

The dynamic nature of e-commerce, fueled by emerging technologies like artificial intelligence (AI), blockchain, and the Internet of Things (IoT), adds further complexity to data protection and privacy concerns [14]-[17]. With the advent of personalized shopping experiences, recommendation systems, and real-time data analytics, businesses are now able to track user behavior, preferences, and purchasing habits. While these technologies enable businesses to tailor their offerings, they also increase the risk of invasive data collection, surveillance, and misuse of sensitive customer information. Moreover, third-party service providers, such as payment processors and logistics companies, often have access to customer data, which can lead to additional vulnerabilities if their security measures are not adequately implemented [18]-[21]. This necessitates a holistic and multi-layered approach to data protection, ensuring not only that consumer data is secure [22] but that consumers are aware of how their data is being used and have control over it.

In light of these issues, it is essential to understand the current landscape of data protection and privacy practices in the e-commerce environment, identify the challenges faced by businesses and consumers, and explore the technological and regulatory advancements that aim to address these concerns. This systematic review paper aims to provide an in-depth analysis of the state of data protection and privacy in e-commerce, offering a comprehensive overview of existing solutions, frameworks, and research in this area. Through this review, exploration is done on the effectiveness of current approaches to securing consumer data, identify emerging privacy concerns, and highlight research gaps that need to be addressed in the ongoing evolution of e-commerce security practices. Ultimately, this paper aims to contribute to the broader understanding of data protection and privacy in e-commerce, offering insights into the best practices, technologies, and strategies that can help e-commerce platforms build trust, ensure compliance, and protect the sensitive information of their users.

Specifically, this systematic review aims to synthesize existing research on data protection and privacy in the e-commerce environment. By critically examining current challenges, emerging solutions, and trends, this study seeks to provide a comprehensive overview of the field. The review focuses on three primary objectives: (1) identifying key threats and vulnerabilities associated with data protection in e-commerce, (2) evaluating technological and regulatory measures designed to address these challenges, and (3) outlining future research directions to enhance privacy and security in this critical domain. Through this investigation, the paper intends to support researchers, policymakers, and industry stakeholders in developing robust strategies for safeguarding data in the e-commerce landscape.

2. E-commerce security issues

E-commerce security is a critical aspect of online business operations, as it involves safeguarding sensitive information, financial transactions, and user data from various threats. The sub-sections below offer an extensive discussion of key security issues faced by e-commerce platforms.

2.1. Data breaches and theft

E-commerce platforms store sensitive customer data, including personal details, payment card information, and login credentials [23], [24]. Cybercriminals target these systems to steal this data, often through vulnerabilities like weak encryption, outdated software, or phishing attacks, as shown in Figure 3. Data breaches can lead to identity theft, financial loss, and reputational damage to businesses.

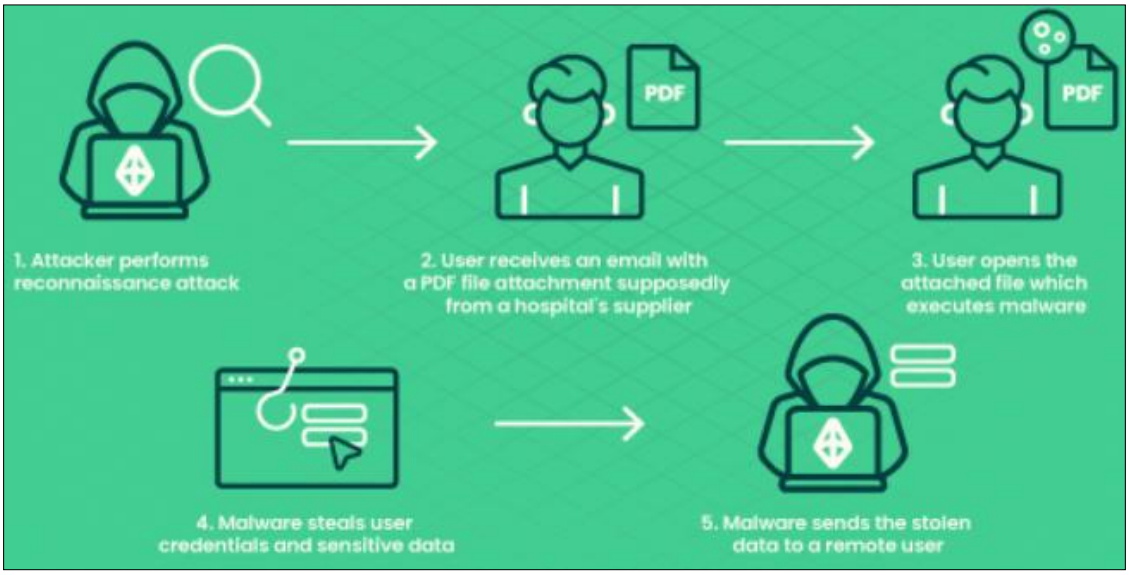

Figure 3 Data breaches and theft

According to [25], data breaches and theft have profound and far-reaching impacts on e-commerce businesses, customers, and the broader digital ecosystem. For businesses, the immediate consequence is financial loss. Breaches often result in hefty fines for failing to comply with data protection regulations like GDPR or PCI DSS [26]. Additionally, businesses face expenses related to breach investigations, legal fees, and compensating affected customers. Beyond direct costs, the loss of customer trust and damage to brand reputation can significantly reduce revenue and market

share. Customers may abandon compromised platforms in favor of competitors, leaving long-term damage to the business's credibility.

For customers, data breaches and theft expose sensitive personal and financial information, such as credit card details, addresses, and login credentials, to malicious actors [27]. This exposure increases the risk of identity theft and fraudulent transactions, potentially causing severe financial and emotional distress. The erosion of customer confidence in the security of e-commerce platforms can lead to a more cautious online shopping culture, reducing overall growth in the e-commerce industry. Additionally, breaches have broader societal implications, as stolen data is often sold on the dark web or used in further cybercrimes, fueling a cycle of digital insecurity [28]. Addressing these impacts requires robust security measures, transparent communication with stakeholders, and efforts to restore trust through accountability and proactive mitigation.

2.2. Payment fraud

Payment fraud is a common issue where attackers exploit online payment systems. Techniques like credit card fraud, chargeback fraud, and fake payment gateways are used to deceive businesses and consumers [29]. The absence of robust fraud detection systems increases the risk of unauthorized transactions.

Payment fraud in e-commerce has significant financial and operational impacts on businesses, as it directly affects revenue and profitability. Fraudulent activities, such as credit card fraud, chargeback fraud, and account takeovers, result in unauthorized transactions and financial losses for merchants [30], [31]. Chargebacks, in particular, impose double costs on businesses—losing the sale and paying additional fees to payment processors. Over time, repeated fraud incidents can lead to higher operating costs, increased scrutiny from payment processors, and even restrictions on payment services if fraud rates exceed acceptable limits. These financial losses are compounded by the need to invest in fraud prevention systems, which can be costly but essential to mitigate future risks.

For customers, payment fraud erodes trust in e-commerce platforms, making them wary of sharing sensitive financial information online. Victims of fraud may face temporary or permanent financial damage, as well as the inconvenience of resolving disputes and recovering funds. On a broader scale, payment fraud undermines the growth of e-commerce by creating a perception of insecurity. This can discourage new users from adopting online shopping and reduce overall consumer confidence. Additionally, the rise of fraud contributes to the demand for more stringent regulatory measures, increasing compliance burdens for businesses. Addressing payment fraud requires a combination of advanced fraud detection tools [32], secure payment gateways, and customer education to create a safer e-commerce environment for all stakeholders.

2.3. Phishing and social engineering

Phishing involves tricking users into revealing their login credentials or other sensitive information by creating fake websites or sending deceptive emails [33], [34], as illustrated in Figure 4. On the other hand, social engineering attacks exploit human psychology to bypass security measures, posing a significant threat to e-commerce security.

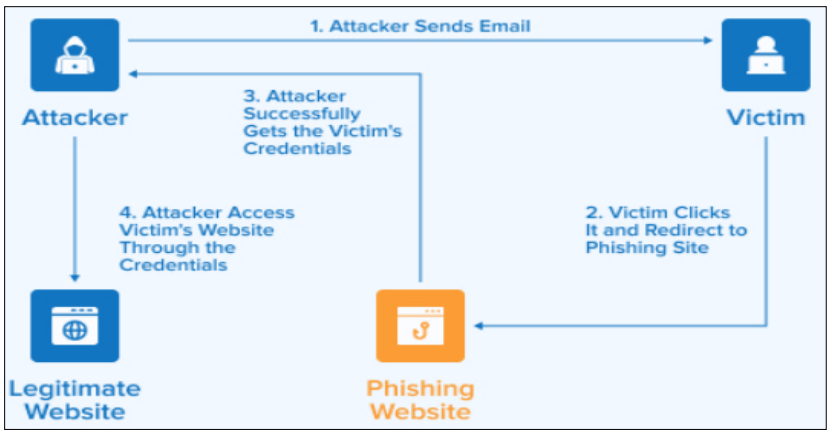

Figure 4 Phishing threat

According to [35], phishing and social engineering (shown in Figure 5) have a severe impact on e-commerce by exploiting human vulnerabilities to compromise sensitive information. Cybercriminals use deceptive tactics, such as

fake emails, websites, or messages, to trick users into revealing login credentials, payment details, or other personal information [36].

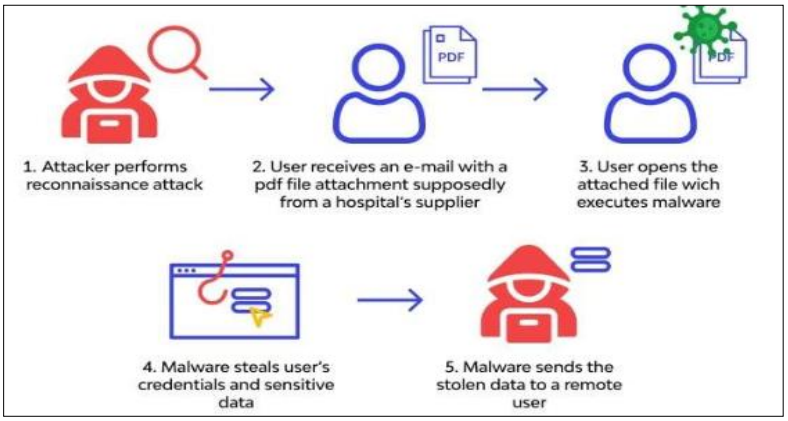

Figure 5 Social engineering attack

For e-commerce platforms, phishing can lead to unauthorized access [37] to customer accounts, resulting in fraudulent transactions and the theft of sensitive data. These incidents damage a company's reputation and undermine customer trust, potentially driving customers to competitors who offer stronger security. Additionally, businesses may face financial losses from fraud, legal consequences due to data protection breaches, and increased costs for implementing security measures.

For customers, phishing and social engineering attacks can lead to identity theft, financial loss, and a sense of insecurity when engaging in online transactions [39]. Victims may find their accounts hijacked, funds stolen, or personal information used in further fraudulent activities. Beyond individual losses, such attacks erode overall confidence in e-commerce platforms, making consumers hesitant to shop online [39]. This creates a challenging environment for businesses, which must continuously invest in customer education, awareness campaigns, and robust anti-phishing tools to mitigate risks. Proactively addressing these threats is essential to fostering a secure and trustworthy online shopping ecosystem.

2.4. Distributed Denial of Service (DDoS) attacks

DDoS attacks aim to overwhelm e-commerce websites with excessive traffic, causing disruptions or complete outages, as shown in Figure 6. These attacks not only affect sales and revenue but also damage customer trust and loyalty.

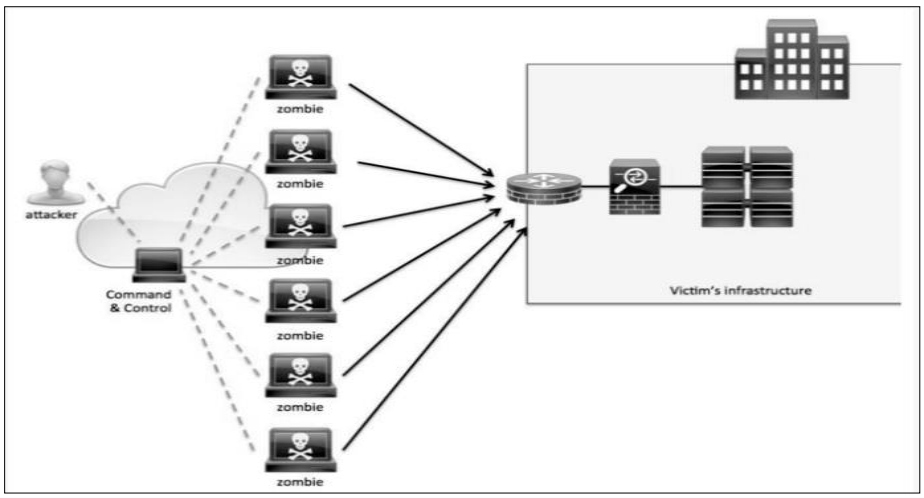

Figure 6 DDoS attack

As explained by [40], DDoS attacks can have a devastating impact on e-commerce platforms by disrupting their availability and functionality. These attacks flood servers with excessive traffic, overwhelming resources and causing

websites or applications to become slow, unresponsive, or completely inaccessible [42], [43]. For e-commerce businesses, this translates into immediate revenue loss, as customers cannot browse, purchase, or interact with the platform. Beyond the financial impact, prolonged or repeated DDoS attacks can severely damage brand reputation, as customers perceive the business as unreliable [44]. Additionally, recovery costs for mitigating the attack, restoring normal operations, and implementing preventive measures can be substantial.

The effects of DDoS attacks extend beyond financial loss to customer trust and loyalty. Customers who experience disrupted services are likely to turn to competitors, and they may hesitate to return even after the platform is restored. For smaller businesses, a single prolonged DDoS attack can be particularly devastating, as they often lack the resources to recover quickly. On a broader scale, such attacks can affect supply chains, disrupt partnerships, and strain relationships with payment processors and third-party vendors [45]. To combat DDoS threats, e-commerce businesses must invest in scalable infrastructure, deploy robust network security solutions like web application firewalls (WAFs) [46], [47], and collaborate with security providers to implement real-time monitoring and mitigation strategies.

2.5. Malware and ransomware

Malware and ransomware attacks target e-commerce websites by infecting servers, stealing data, or locking critical systems until a ransom is paid [48], as shown in Figure 7. These attacks can compromise the integrity and availability of online stores.

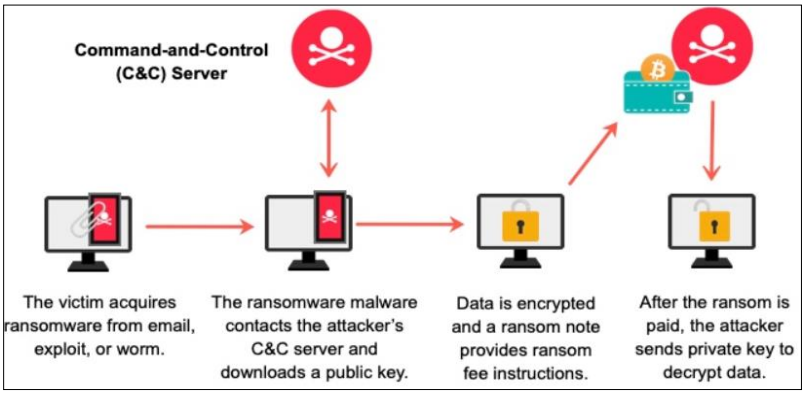

Figure 7 Malware and ransomware threats

Malware and ransomware pose significant threats to e-commerce platforms, compromising their operations, data integrity, and customer trust [49]. Malware, such as keyloggers or spyware, infiltrates systems to steal sensitive information like payment details, customer credentials, and business data [50]. Ransomware takes this a step further by encrypting critical files or systems and demanding payment for their release [51]. For e-commerce businesses, such attacks can halt operations, leading to immediate revenue loss and disruption of services. The costs of resolving these attacks, including paying ransoms, recovering data, and implementing security upgrades [52], can be overwhelming, especially for smaller businesses. Additionally, data breaches resulting from malware can lead to legal penalties for failing to comply with data protection regulations, further increasing financial and reputational damage.

For customers, malware and ransomware attacks erode confidence in the safety of online shopping [53]. Customers affected by these breaches may experience identity theft, fraudulent transactions, or unauthorized access to their accounts. Such incidents can deter consumers from engaging with e-commerce platforms perceived as vulnerable, impacting the overall growth of the sector. The broader implications include the proliferation of stolen data on the dark web, fueling other cybercrimes. To mitigate these risks, e-commerce businesses must adopt a multi-layered security approach, including real-time malware detection, endpoint protection, and regular system updates [54], [55]. Proactive measures like educating employees and customers about phishing and securing data backups are essential to minimize the impact of these pervasive threats.

2.6. Weak authentication mechanisms

Inadequate authentication methods, such as relying solely on passwords, make it easier for attackers to gain unauthorized access [56]. Weak or reused passwords are particularly vulnerable to brute-force or credential-stuffing attacks.

Weak authentication mechanisms in e-commerce significantly undermine the security of online transactions, making it easier for attackers to gain unauthorized access to customer accounts and sensitive data [57], [58]. Passwords that are easily guessable or reused across platforms increase vulnerability to brute-force attacks and credential-stuffing attempts. Cybercriminals exploiting these weaknesses can hijack accounts, conduct fraudulent transactions, or steal personal and payment information. For e-commerce businesses, such breaches result in financial losses from chargebacks, reimbursements, and fraud-related fees [59]. Beyond monetary costs, these incidents damage customer trust, tarnish brand reputation, and may lead to legal consequences for failing to safeguard user data.

From the customer's perspective, weak authentication mechanisms expose them to identity theft, financial fraud, and account takeovers [60], which can cause significant financial and emotional distress. Affected customers may lose confidence in online shopping, turning to competitors or avoiding e-commerce altogether. On a larger scale, weak authentication contributes to the perception that online platforms are unsafe, hindering the growth of the e-commerce industry [61]. To address these issues, businesses must implement stronger authentication methods, such as multi-factor authentication, biometric verification, and advanced fraud detection systems [62]. Educating users about creating strong passwords and recognizing phishing attempts is equally critical to fortifying overall e-commerce security.

2.7. Third-party vulnerabilities

Many e-commerce platforms rely on third-party plugins, payment gateways, or software integrations [63]. As shown in Figure 8, vulnerabilities in these third-party components can serve as entry points for attackers to compromise the entire system.

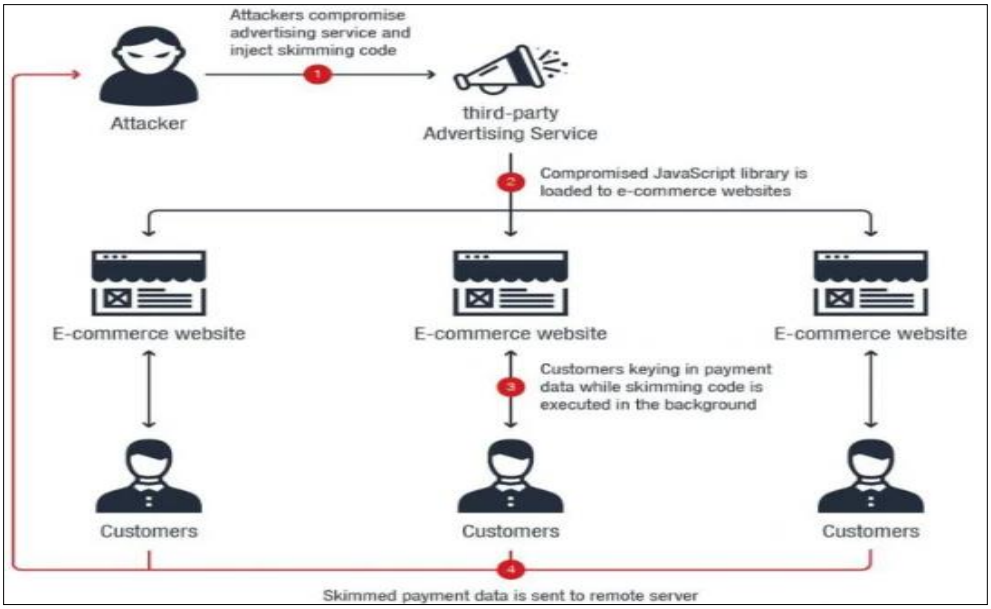

Figure 8 Third-party vulnerabilities

Third-party vulnerabilities present a significant risk to e-commerce platforms, as many businesses rely on external vendors for various services, including payment processing, customer support, and website functionality [64], [65]. If a third-party service provider experiences a security breach or has a vulnerability in their systems, it can serve as an entry point for attackers to compromise the e-commerce platform. For example, a vulnerability in a payment gateway or plugin can expose customer payment details, leading to financial losses, fraud, and data theft. Additionally, security lapses in third-party tools that handle customer data can result in data breaches [66], violating privacy regulations and causing legal consequences for the e-commerce business.

The impact on e-commerce businesses is twofold—direct and reputational. Beyond the immediate financial losses and potential legal penalties, a breach stemming from a third-party vulnerability can cause long-term damage to customer trust [67], [68]. Customers expect e-commerce platforms to ensure the safety of their data, regardless of where it is processed or stored. When third-party systems fail, businesses can lose customer confidence, resulting in a decline in sales and a damaged reputation. To mitigate these risks, e-commerce businesses must rigorously vet third-party providers, ensure their security standards meet industry regulations, and maintain strong oversight of the external

services they integrate with. Regular security assessments, contractual agreements, and clear incident response plans with third-party vendors are essential to minimizing the impact of third-party vulnerabilities.

2.8. Insecure communication channels

Failure to use secure protocols like HTTPS can expose sensitive data to interception during transmission. Man-in-the-middle (MITM) attacks (shown in Figure 9) can exploit insecure connections to intercept and modify data between users and the platform [69].

Insecure communication channels in e-commerce expose both businesses and customers to significant risks, primarily through the interception of sensitive data [70]- [72]. When communication between users and e-commerce platforms is not properly encrypted, attackers can engage in man-in-the-middle (MITM) attacks, intercepting data such as login credentials, payment information, and personal details [73]. Without encryption protocols like HTTPS or SSL/TLS, these sensitive transactions can be easily compromised, leading to data breaches and financial fraud [74]. For businesses, this vulnerability can result in immediate losses from fraudulent transactions, fines for failing to comply with data protection regulations, and long-term reputational damage.

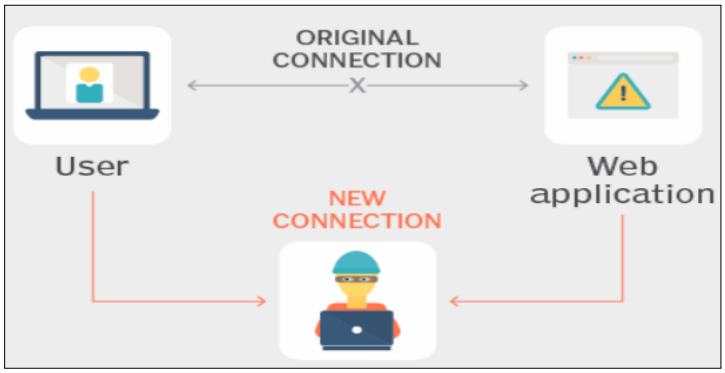

Figure 9 MITM attack

For customers, insecure communication channels create a feeling of insecurity when interacting with online stores, leading to a loss of confidence in e-commerce platforms. If personal and financial data is exposed or stolen, customers may suffer identity theft, unauthorized purchases, and account hijacking, which can lead to both financial and emotional distress [75], [76]. The overall impact is a decline in consumer trust in online transactions, which can deter new users from engaging with e-commerce sites and reduce overall market growth. To protect both businesses and consumers, e-commerce platforms must enforce the use of secure communication protocols, implement end-to-end encryption, and regularly audit their systems to ensure secure data transmission throughout the customer experience.

2.9. Session hijacking

Attackers can steal session cookies to impersonate users, gaining unauthorized access to accounts or sensitive information [77]. Inadequate session management and lack of encryption exacerbate this issue. Session hijacking can have a severe impact on e-commerce platforms by compromising user accounts and allowing unauthorized access to sensitive information [78], as demonstrated in Figure 10. Attackers exploit weaknesses in session management, such as stealing session cookies or exploiting insecure authentication mechanisms [79], [80].

Once an attacker gains control of a session, they can impersonate legitimate users, performing actions such as making fraudulent purchases, altering personal information, or transferring funds. This not only results in financial losses for the business but also damages customer trust, as users may lose confidence in the security of the platform. For businesses, the recovery costs from these breaches, such as investigation expenses and securing affected accounts, can be significant, and brand reputation may take years to repair.

From the customer's perspective, session hijacking can lead to identity theft, unauthorized access to accounts, and misuse of personal and payment information [81]. Victims of session hijacking may experience financial fraud, unauthorized transactions, and the inconvenience of recovering compromised accounts. The broader impact is a decline in trust in e-commerce systems, with customers becoming more cautious about online transactions. This reduces the growth of e-commerce, as potential users may shy away from using platforms that appear vulnerable. To mitigate the risk of session hijacking, e-commerce businesses should implement secure session management practices, such as using

HTTPS, employing strong encryption methods, and regularly rotating session keys to prevent unauthorized access [82]-[84]. Additionally, multi-factor authentication can add an extra layer of security by requiring more than one form of verification for account access.

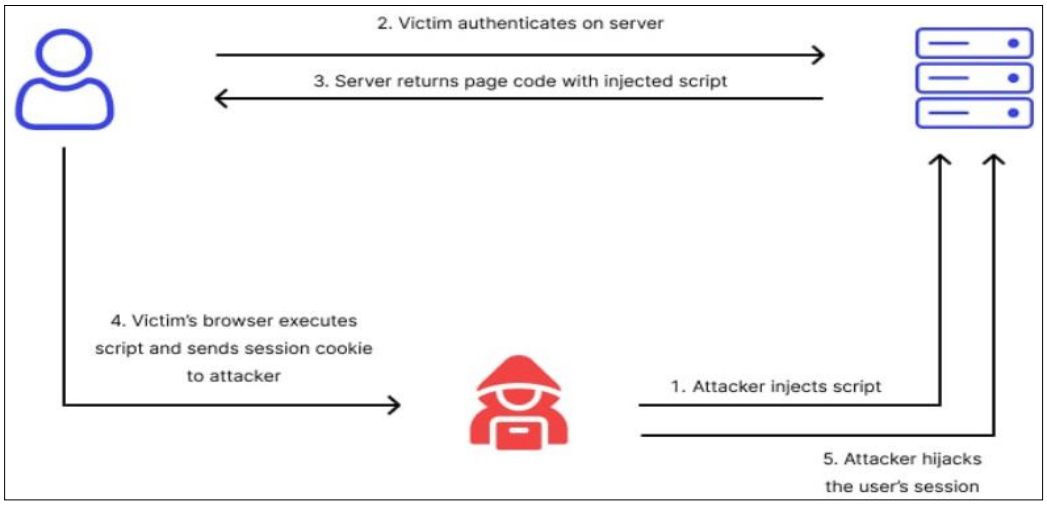

Figure 10 Session hijacking threat

2.10. SQL Injection and Cross-Site Scripting (XSS)

SQL injection attacks exploit vulnerabilities in a website's database query logic, allowing attackers to manipulate or retrieve sensitive data [85], [86], as illustrated in Figure 11. Similarly, XSS attacks (shown in Figure 12) inject malicious scripts into web pages, compromising user sessions and stealing information.

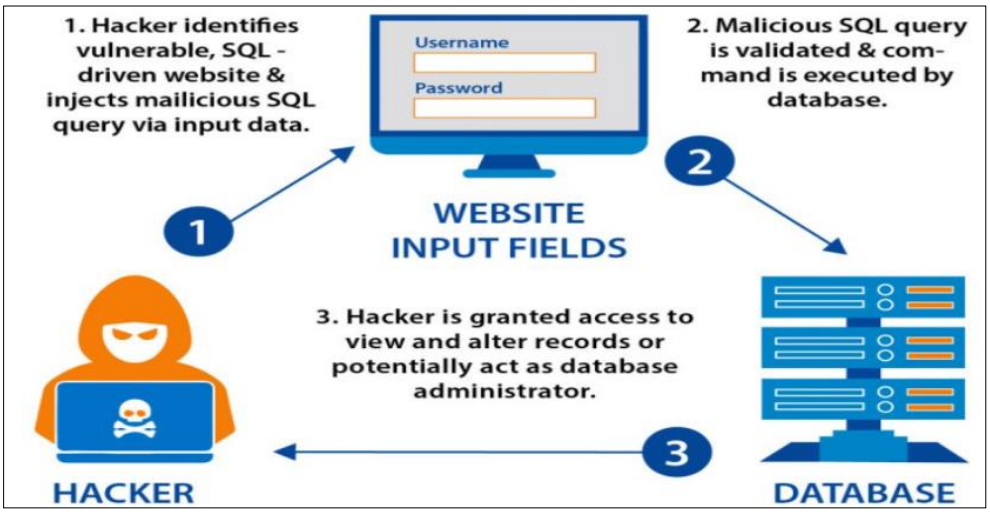

Figure 11 SQL injection attack

SQL injection and cross-site scripting attacks represent significant security threats to e-commerce platforms, with the potential to compromise both customer data [87] and system integrity. SQL injection occurs when an attacker manipulates input fields in order to execute malicious SQL queries on the backend database, often gaining unauthorized access to sensitive customer data, such as payment details, addresses, and login credentials [88], [89].

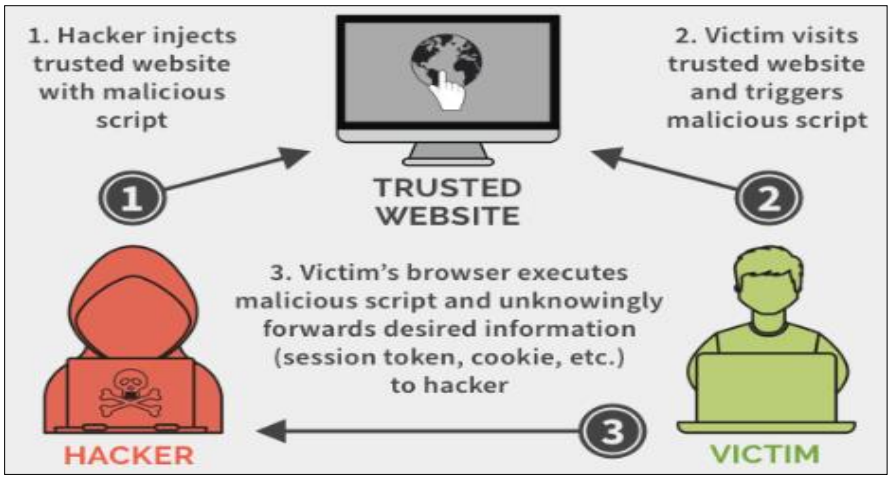

Figure 12 Cross-Site Scripting

This can result in massive data breaches, financial fraud, and legal liabilities for businesses that fail to secure their databases. XSS, on the other hand, involves injecting malicious scripts into a website's code, which then executes when users interact with the compromised web page [90], [91]. This can lead to session hijacking, defacement of web content, and the theft of user data, including cookies or login credentials.

The impact of these attacks on e-commerce platforms extends beyond financial loss to include significant reputational damage and erosion of customer trust. If customers learn that their personal information or payment details have been compromised due to vulnerabilities like SQL injection or XSS, they may abandon the platform and seek safer alternatives. This can lead to a decline in sales, reduced user engagement, and loss of market share. For businesses, recovery from such attacks often involves legal costs, regulatory fines, and the need for extensive system overhauls to secure their infrastructure. To protect against these threats, e-commerce sites must implement secure coding practices, regularly test for vulnerabilities, and deploy security measures such as input validation, web application firewalls, and content security policies (CSPs) [92], [93] . By addressing these vulnerabilities, businesses can prevent attackers from exploiting weak points in their systems and safeguard both customer data and platform integrity.

2.11. Insider threats

Employees or contractors with access to critical systems may misuse their privileges, either intentionally or inadvertently, leading to data leaks or security breaches [94]. Figure 13 gives a depiction of a typical insider threat. Insider threats in e-commerce pose significant risks, as employees or contractors with authorized access to systems and data can exploit their privileges to steal sensitive information or sabotage operations [95]. These threats may come from disgruntled employees who intentionally leak customer data, alter transactional records, or even execute fraud through administrative accounts.

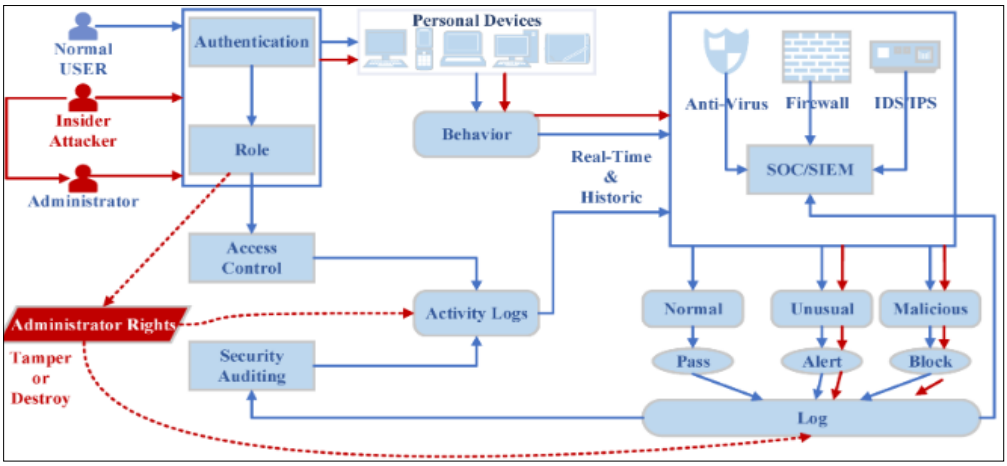

Figure 13 Insider threats

The consequences of such breaches are far-reaching, as businesses may experience financial loss due to fraud, unauthorized transactions, or data theft. Insider threats can also disrupt the platform's operations, leading to service outages, data corruption, and loss of customer trust [96]. Additionally, the legal and regulatory consequences of failing to safeguard sensitive data from insiders can result in fines, lawsuits, and compliance violations.

The impact on customers is equally severe, as personal and financial information may be exposed, leading to identity theft, fraudulent charges, and a loss of privacy. A single insider breach can tarnish a business's reputation, making customers hesitant to engage with the platform, especially if their trust in data security is compromised [97]. Long-term effects include a decrease in customer retention, reduced sales, and the potential to lose market share to competitors with more secure platforms. To mitigate the risks of insider threats, e-commerce businesses must enforce strict access controls, conduct background checks on employees, and implement continuous monitoring and auditing systems [98], [99]. Additionally, fostering a culture of security awareness and offering employees proper training on handling sensitive data can help prevent and identify potential insider threats before they cause significant harm.

3. Probable solutions

Addressing security challenges in e-commerce is crucial to ensuring a safe, trustworthy, and resilient platform for both businesses and customers. Implementing robust security measures helps mitigate various threats, such as data breaches, fraud, and cyberattacks, while maintaining compliance with regulatory requirements. The following are some comprehensive solutions to the security challenges faced by e-commerce platforms:

3.1. Data encryption and secure communication

One of the foundational solutions to securing e-commerce systems is ensuring that all data transmitted between users and the platform is encrypted [100], as illustrated in Figure 14. Using secure communication protocols like HTTPS and SSL/TLS ensures that sensitive customer information, such as personal details, credit card numbers, and login credentials, cannot be intercepted by malicious actors during transmission [102], [103].

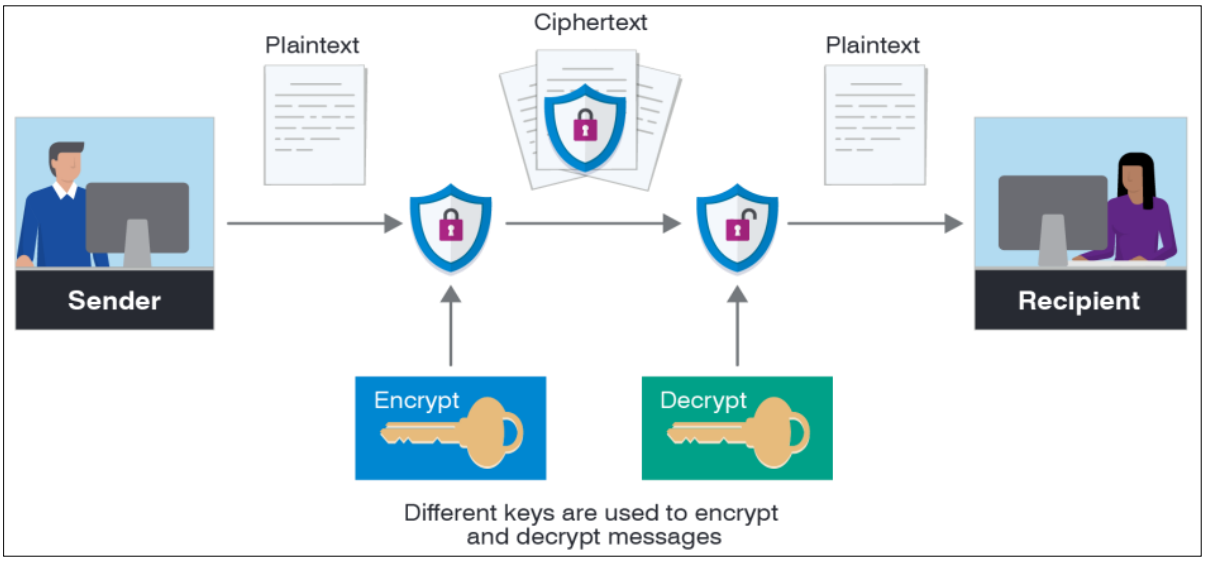

Figure 14 Data encryption

Implementing encryption for data at rest, such as storing customer information in encrypted databases, further protects against data theft in the event of a breach [104], [105]. E-commerce businesses should regularly update their encryption methods and ensure compliance with industry standards to minimize vulnerabilities.

3.2. Multi-Factor Authentication (MFA)

To prevent unauthorized access to user accounts, e-commerce platforms should implement multi-factor authentication (MFA), which requires users to verify their identity through multiple methods beyond just passwords [106], [107]. As shown in Figure 15, MFA could include SMS or email verification, biometrics (e.g., fingerprints or facial recognition), or authenticator apps.

Figure 15 Multi-Factor Authentication

This additional layer of security makes it significantly harder for attackers to access accounts, even if they obtain login credentials through phishing, data breaches, or brute-force attacks [108], [109]. MFA can also be implemented for administrative accounts to ensure that sensitive business data is not easily accessed or manipulated by malicious actors.

3.3. Strong password policies and encryption

A fundamental yet often overlooked solution is enforcing strong password policies that require users to create complex, unique passwords [110]. E-commerce platforms should encourage or mandate the use of long, alphanumeric passwords with special characters, combined with periodic password changes [111]. Implementing password hash encryption, where passwords are stored in a non-reversible form, further ensures that even if an attacker gains access to the database, they cannot easily retrieve the original passwords. For added security, platforms should also educate users about avoiding password reuse across different websites, a common vulnerability [112] exploited in credential-stuffing attacks.

3.4. Fraud detection and prevention systems

E-commerce businesses should integrate fraud detection systems to monitor transactions in real-time and identify suspicious patterns [113]. Machine learning-based solutions can be used to detect anomalies such as unusual purchase amounts, multiple failed login attempts, or changes in buying behavior [114]. As shown in Figure 16, advanced fraud detection systems can flag or block high-risk transactions and notify administrators, reducing the likelihood of fraud and chargebacks [115].

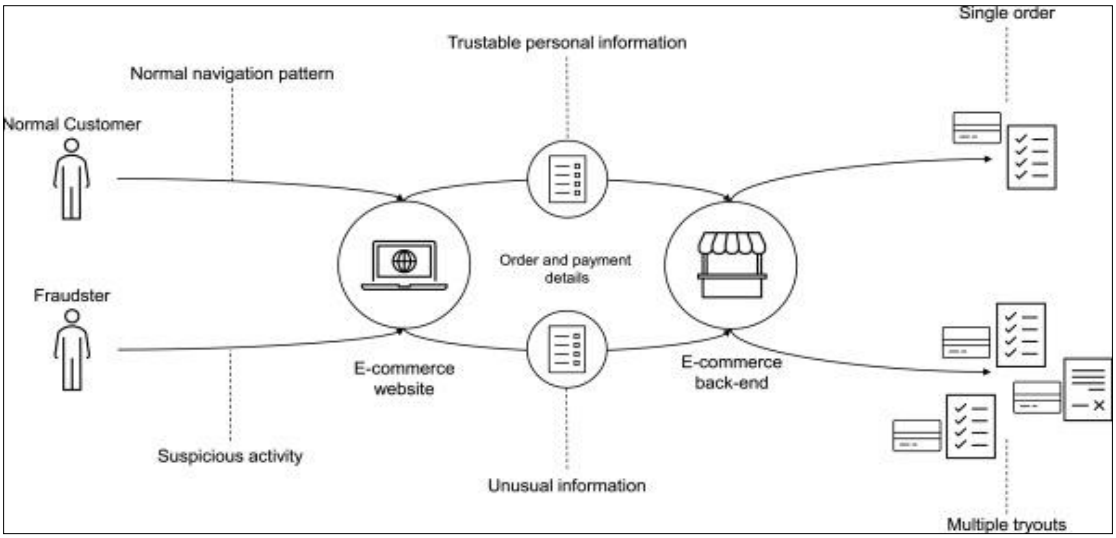

Figure 16 Fraud detection and prevention

Integrating with trusted payment gateways that offer built-in fraud protection features, like 3D Secure or Verified by Visa, can also prevent unauthorized payments from going through. Regular updates and refinements to fraud detection algorithms are essential to keeping up with evolving threats.

3.5. Web Application Firewalls (WAFs) and anti-malware solutions

Web application firewalls are vital in defending e-commerce platforms against common cyberattacks like SQL injection, cross-site scripting, and cross-site request forgery (CSRF) [116]. As shown in Figure 17, WAFs filter and monitor HTTP traffic, blocking malicious requests [117] before they reach the web server. Anti-malware solutions, including antivirus software and endpoint protection tools, should also be deployed to detect and neutralize any malicious code or ransomware that may attempt to infiltrate the system [118], [119]. Keeping these security tools up to date is vital, as cybercriminals frequently exploit new vulnerabilities to bypass defenses.

3.6. Regular security audits and vulnerability assessments

Frequent security audits and vulnerability assessments are essential for identifying and addressing potential weaknesses in the platform's architecture, applications, and infrastructure [120], [121]. Penetration testing, conducted by security professionals, simulates real-world attacks to identify vulnerabilities [122] in the system before malicious actors can exploit them. Businesses should also conduct regular software updates and patch management to address known vulnerabilities in third-party tools, plugins, and frameworks [123].

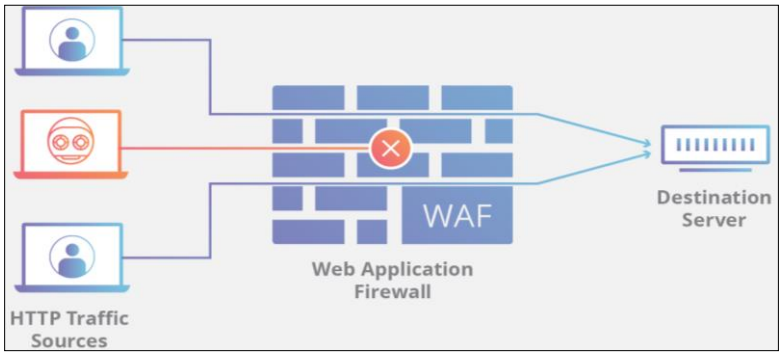

Figure 17 Web Application Firewall

Integrating security testing into the development lifecycle (DevSecOps) helps ensure that security is considered at every stage of software development.

3.7. Data privacy regulations and compliance

E-commerce platforms must ensure they comply with global data privacy regulations such as the General Data Protection Regulation, California Consumer Privacy Act, and the Payment Card Industry Data Security Standard (PCI DSS) [124], [125]. Adhering to these regulations not only ensures legal compliance but also builds consumer trust by demonstrating a commitment to data privacy. Regular compliance audits and encryption of sensitive customer data are required to protect against breaches and avoid penalties [126], [127]. E-commerce businesses should also establish clear data handling policies and implement systems for customer consent management, ensuring users are informed about how their data is used and processed.

3.8. User education and awareness

One of the most effective ways to prevent security breaches, particularly phishing and social engineering attacks, is through user education. E-commerce businesses should provide customers with clear guidelines on recognizing phishing attempts [128], the importance of creating strong passwords [129], and how to secure their devices when making online purchases [130]. Regular customer awareness campaigns, pop-up tips during checkout, and emails with security reminders can help reduce the success rate of attacks. Employees should also be trained in recognizing common security threats to avoid becoming unwitting participants in social engineering schemes.

3.9. Secure payment gateways and tokenization

To reduce the risks associated with online payments, businesses should use secure, PCI DSS-compliant payment gateways that provide secure methods for handling transactions [131]. As demonstrated in Figure 18, tokenization, which replaces sensitive payment information (such as credit card numbers) with a unique identifier or token, can minimize exposure of critical payment data [132]. In the event of a breach, tokens cannot be used to process fraudulent transactions, reducing the severity of any compromise. Additionally, adopting 3D Secure technology (e.g., Visa's Verified

by Visa) [133] adds an extra layer of security during payment transactions by requiring additional verification from the customer, such as a one-time password or biometric authentication.

3.10. Incident response and recovery plans

Despite all preventive measures, e-commerce platforms must be prepared for the worst by having a comprehensive incident response plan [134], [135]. In the event of a security breach, businesses must be able to quickly identify the nature of the attack, contain it, and notify affected users. A recovery plan should include data backup strategies, disaster recovery processes, and measures for restoring normal operations [136]. Regular drills should be conducted to ensure all stakeholders know their roles and responsibilities during an incident. Transparent communication with customers is also essential, as informing them promptly can help mitigate damage to reputation and rebuild trust.

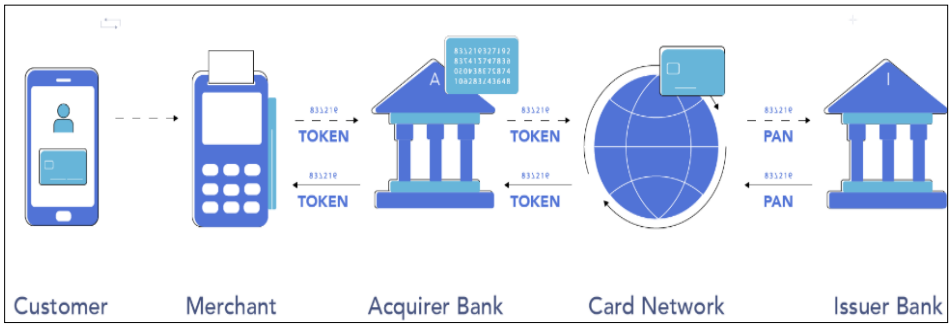

Figure 18 Tokenization

In a nutshell, adopting a multi-layered approach that combines these solutions, e-commerce businesses can greatly reduce the likelihood of cyberattacks, fraud, and data breaches. Securing both the platform and customer data requires a combination of advanced technologies, vigilant monitoring, robust encryption [137], and continuous education. Implementing a strong security framework [138] will not only protect sensitive information but also ensure the longevity of the e-commerce business by maintaining customer trust and ensuring smooth operations in a rapidly evolving digital landscape.

4. Issues with current solutions

While current e-commerce security solutions have made significant advancements in protecting online platforms, they still face several challenges that can hinder their effectiveness. These challenges stem from the evolving nature of cyber threats, the complexity of e-commerce environments, and the increasing sophistication of attackers. Below is an in-depth look at some of the key challenges faced by current e-commerce security solutions:

4.1. Evolving and sophisticated cyberattacks

One of the major challenges for e-commerce security is the continuous evolution of cyber threats [139]. Cybercriminals are becoming more sophisticated in their tactics, using advanced tools and techniques to bypass traditional security measures. Attacks such as distributed denial of service [140], SQL injection [141], Cross-Site Scripting [142], and ransomware [143] are constantly being refined, making it difficult for existing security systems to keep up. Attackers now employ machine learning, AI-driven bots, and other advanced methods to automate attacks, target specific vulnerabilities, and scale attacks in ways that challenge existing defenses [144]. As a result, e-commerce businesses must continuously adapt their security strategies, conduct regular penetration testing, and implement advanced threat detection systems that can identify and respond to new attack vectors.

4.2. Integration of multiple third-party services

E-commerce platforms often rely on third-party services such as payment gateways, cloud hosting providers, and marketing platforms to enhance user experience and streamline operations [145]. While these integrations offer benefits, they also create significant security challenges. A vulnerability in a third-party service can open doors for attackers to compromise the entire e-commerce platform [146]. For example, a flaw in a payment processor could expose customers' financial data, while a security breach [147] in a cloud service could lead to unauthorized access to sensitive business or customer information. Managing the security of these third-party systems requires ongoing monitoring, regular security assessments, and strong contractual agreements that ensure third-party providers adhere

to best practices in cybersecurity. However, even with these precautions, e-commerce platforms are still vulnerable to the risks posed by insecure third-party integrations.

4.3. Complexity in securing customer data

As e-commerce platforms store large volumes of sensitive customer data, including personal details, credit card numbers, and purchase histories, securing this information has become an increasingly complex task [148], [149]. Even with encryption and secure storage solutions, businesses face difficulties in ensuring that data is protected at all stages—whether at rest, in transit, or during processing. Security issues arise due to inconsistent or poorly implemented encryption techniques, as well as the lack of visibility into how and where customer data is stored and accessed [150]-[152]. Furthermore, businesses must comply with various privacy regulations, such as GDPR, CCPA, and PCI DSS, which create additional complexities in how data is handled, stored, and shared. Ensuring compliance with these regulations while maintaining robust security controls can be challenging, especially as e-commerce businesses scale and expand their operations globally.

4.4. User behavior and social engineering attacks

Despite the implementation of advanced security measures, human error remains one of the weakest links in e-commerce security [153], [154]. Phishing, social engineering, and other manipulation tactics continue to be highly effective in gaining unauthorized access to customer accounts or business systems. Users may fall victim to phishing attacks that trick them into revealing login credentials or personal information [155], or employees may be duped into clicking on malicious links that lead to malware infections [156]. Additionally, weak password practices and the reuse of credentials across multiple platforms make it easier for attackers to execute credential-stuffing attacks. Even with multi-factor authentication in place, attackers may still find ways to circumvent these protections through tactics such as SIM swapping or exploiting poor user behavior. E-commerce businesses must invest in educating users, continuously monitoring for suspicious behavior, and incorporating more advanced user verification methods [157] to combat social engineering attacks.

4.5. Lack of real-time threat detection and response

One of the key limitations of many current e-commerce security solutions is the inability to detect and respond to threats in real time. Many traditional security systems rely on signature-based detection methods [158] that identify known threats, but they are less effective against zero-day attacks [159] or novel attack vectors. As attackers become more adept at hiding their activities, there is a growing need for more sophisticated, proactive monitoring solutions [160] that can detect anomalies in real-time, predict potential threats, and respond automatically before damage occurs. The challenge lies in the high volume of data generated by e-commerce platforms, which makes it difficult for security teams to manually review and detect subtle patterns indicative of a security breach. Machine learning and artificial intelligence-based security solutions [162], [163] offer promise in addressing this issue, but they still face challenges in achieving high accuracy and reducing false positives.

4.6. Securing mobile and IoT devices

The increasing use of mobile devices and internet of things products for e-commerce transactions presents new security challenges [163]. Mobile devices are particularly vulnerable to threats such as malware, data theft, and unauthorized access through unsecured Wi-Fi networks [164]. Furthermore, e-commerce platforms must account for the variety of devices, operating systems, and browsers used by customers, which increases the attack surface [165]. IoT devices, such as smart home devices or connected wearables, are also becoming more integrated into e-commerce environments, often collecting and transmitting sensitive user data [166], [167]. These devices can be entry points for cybercriminals if not properly secured, especially if they have weak authentication mechanisms or outdated firmware. As e-commerce businesses extend their services to mobile and IoT platforms, they must ensure that all devices are securely connected, data is encrypted, and access is appropriately managed.

4.7. Compliance and regulatory challenges

Compliance with evolving data protection regulations is an ongoing challenge for e-commerce businesses [168]. Different regions and jurisdictions have different requirements for how businesses must protect customer data, with regulations such as GDPR, CCPA, and PCI DSS imposing strict security measures to safeguard personal and payment information. Failing to comply with these regulations can result in hefty fines, legal liability, and reputational damage. However, staying compliant while maintaining a flexible, dynamic security posture is difficult [169], as businesses must continuously monitor changing laws, update their security protocols, and ensure their systems meet global standards.

Additionally, regulations such as the GDPR require businesses to provide customers with greater control over their data [170], creating complexities in data handling, storage, and deletion that must be integrated into security strategies.

4.8. Scalability and cost of security solutions

As e-commerce businesses grow, they face the challenge of scaling their security solutions to meet the demands of a larger customer base, higher traffic volumes, and more complex systems [171]. Traditional security tools may struggle to keep up with the increasing scale, leading to vulnerabilities [172] and inefficiencies. Moreover, investing in robust security solutions that can scale with the business is often cost-prohibitive [173], particularly for small and medium-sized e-commerce businesses. This creates a dilemma for many organizations—how to balance the cost of security with the need for comprehensive protection. Cloud-based security solutions offer some flexibility [174], but they can still be expensive, and ensuring seamless integration with existing systems requires careful planning. Finding cost-effective, scalable security solutions that provide adequate protection for growing businesses remains a major challenge in the e-commerce sector.

4.9. Supply chain and vendor risk management

In an increasingly interconnected e-commerce ecosystem, businesses depend on a range of external suppliers, service providers, and partners to deliver goods and services [175]. However, each third-party vendor introduces potential security risks. A security vulnerability in one of these vendors can cascade through the entire supply chain [176], impacting e-commerce platforms that rely on those services. For instance, a payment processor with weak security could expose a platform to data breaches or fraud, while a logistics partner might inadvertently allow cybercriminals to compromise shipment details. Managing the security risks associated with vendors and ensuring that third parties comply with stringent security standards is an ongoing challenge. E-commerce businesses must conduct regular security assessments and establish clear security protocols [177] and risk management procedures with all suppliers and partners to reduce exposure to third-party vulnerabilities.

4.10. Balancing security with user experience

The e-commerce platforms must find the right balance between robust security and a seamless, user-friendly experience [178]. Security measures such as multi-factor authentication, CAPTCHA verification, and frequent password resets, while necessary, can disrupt the user experience and frustrate customers [179], [180]. A cumbersome or overly complicated security process can drive potential buyers away and reduce conversion rates [181]. Businesses must carefully design their security protocols [182] to protect users without compromising the ease of use and convenience that e-commerce shoppers expect. Striking this balance often requires leveraging advanced technologies, such as biometrics or AI-based fraud detection, to ensure security without interrupting the shopping experience.

Evidently, the challenges faced by current e-commerce security solutions are diverse and ever-evolving, requiring businesses to stay ahead of new threats, adapt to changing regulatory landscapes, and implement a layered approach to defense. While technological advances, such as AI and machine learning, offer promising solutions, human error, third-party vulnerabilities, and the growing complexity of e-commerce environments continue to pose significant risks [183]. Addressing these challenges requires a holistic strategy that includes proactive monitoring, continuous education, robust security protocols, and a commitment to compliance. Only by staying vigilant and adaptable can e-commerce businesses successfully protect themselves and their customers in an increasingly hostile digital world.

5. Research gaps

Despite the numerous advancements in e-commerce security and privacy over the years, significant research gaps still exist, reflecting the dynamic and rapidly evolving nature of both cybersecurity threats and user expectations. These research gaps highlight areas where further exploration is needed to improve the resilience of e-commerce platforms and safeguard customer privacy. The sub-sections that follow give an extensive description of some of the key research gaps in e-commerce security and privacy.

5.1. AI and Machine learning for threat detection

While artificial intelligence and machine learning have made notable strides in enhancing threat detection and response, there are still gaps in effectively leveraging these technologies for e-commerce security. Many current AI-based systems for threat detection struggle with high false-positive rates , which can overwhelm security teams and reduce the effectiveness of these solutions [184], [185]. Additionally, there is a lack of research into developing AI models that can learn from real-time data and predict novel, zero-day attacks. For e-commerce platforms, where fraudsters constantly evolve their tactics, AI systems must be able to adapt rapidly and accurately to new threats [186], [187]. Further

research is needed into developing adaptive, self-learning AI systems that can more effectively detect and neutralize sophisticated attacks in real time, reducing the reliance on pre-configured rules and signatures.

5.2. Privacy-preserving technologies

As data privacy concerns continue to grow, there is an increasing need for research into privacy-preserving technologies that can ensure the confidentiality of sensitive customer information while still enabling businesses to operate effectively [188], [189]. One of the most significant gaps is the development of secure, privacy-preserving data analytics methods, such as differential privacy, which allows organizations to extract insights from data without exposing individual user information [190], [191]. However, there is limited research into how these technologies can be scaled to handle the large volumes of data generated by e-commerce platforms. Furthermore, ensuring that privacy-preserving technologies [192] can be seamlessly integrated into existing e-commerce systems without significantly impacting performance or user experience remains a challenge. More research is needed to create scalable, efficient, and user-friendly privacy solutions that align with both privacy regulations (e.g., GDPR) and business objectives.

5.3. User-centric privacy and security solutions

Most e-commerce security solutions tend to prioritize the protection of the business infrastructure over user-centric privacy and security [193]. While e-commerce businesses deploy various technologies to safeguard their systems, user data is often still exposed to privacy risks due to inadequate user control or understanding of how their data is handled [194], [195]. Research is needed into developing user-centric privacy solutions that empower customers to have more control over their personal information, such as advanced privacy dashboards, granular consent management [196], and transparent data usage notifications. Furthermore, studies are required on how to create user-friendly, customizable security features that do not alienate users or add friction to the purchasing experience. Ensuring that customers can actively manage their data preferences while maintaining a smooth, convenient shopping experience is an area that remains underexplored.

5.4. Secure payment systems and tokenization

While many e-commerce platforms employ secure payment methods like tokenization and encryption, there is still limited research into how these systems can be improved, particularly with regard to mitigating fraud and ensuring seamless user experiences. Research is needed to explore more advanced tokenization methods [197] that enhance security by reducing the risk of token theft or misuse during payment transactions. Additionally, the integration of blockchain technology in payment systems remains an area of interest. Blockchain's inherent security features, such as decentralization and immutability, could provide a more secure and transparent way to handle online payments [198], [199], but further investigation is required to address scalability, latency, and integration challenges with existing payment systems. Research is also needed to enhance the usability and security of digital wallets, cryptocurrencies, and other emerging payment methods, ensuring that they are both secure and accessible to a broad audience.

5.5. Threats to mobile and IoT in E-commerce

With the rise of mobile commerce and internet of things devices, new security and privacy risks have emerged that require further investigation [200], [201]. The research into securing mobile commerce transactions and IoT devices remains limited in comparison to desktop or traditional e-commerce systems. Mobile devices, in particular, are vulnerable to malware, spyware, and other types of attacks due to their smaller screen sizes, user convenience features, and reliance on mobile networks. Research is needed to explore mobile-specific security vulnerabilities and how they can be mitigated through more effective encryption, secure authentication methods [202], and malware detection. Similarly, the IoT ecosystem, which is increasingly integrated into e-commerce platforms through connected products, raises privacy concerns about continuous data collection, tracking, and unauthorized access [203]. Research should focus on improving the security of IoT devices used in e-commerce, with particular emphasis on ensuring secure data transmission, device authentication, and access control.

5.6. Blockchain and distributed ledger technology for e-commerce security

Blockchain and distributed ledger technology offer promising solutions for securing transactions and ensuring the integrity of data in e-commerce [204], [205]. However, research into practical applications of these technologies for e-commerce security is still in its infancy. While blockchain has been touted for its potential to prevent fraud, reduce chargebacks, and improve transparency in supply chains, there are several challenges to overcome. For instance, scalability remains a key issue, as blockchain networks struggle to handle the high transaction volumes typical of e-commerce platforms [206]. Additionally, the cost and energy requirements of certain blockchain implementations are concerns. Further research into energy-efficient blockchain systems, sharding techniques for scalability, and the

integration of blockchain with existing e-commerce platforms is necessary to fully harness its potential in e-commerce security.

5.7. Behavioral biometrics for authentication

While traditional authentication methods such as passwords and multi-factor authentication are effective to some extent, they are often vulnerable to social engineering and credential theft [207], [208]. Behavioral biometrics, which analyzes patterns in user behavior such as typing speed, mouse movements, and navigation habits, presents an innovative solution to enhance authentication security [209]. However, the adoption of behavioral biometrics in e-commerce is still limited due to several challenges, including accuracy, privacy concerns, and the cost of implementation. Research is needed to improve the accuracy and reliability of behavioral biometrics systems, develop standards for integrating them into existing authentication processes, and address the privacy issues that arise from the collection of detailed behavioral data [210]. Further exploration is required to determine the optimal combination of behavioral biometrics and traditional methods for secure, user-friendly authentication.

5.8. Privacy and security of data analytics in e-commerce

Data analytics plays a crucial role in e-commerce for personalizing user experiences, optimizing inventory, and driving targeted marketing campaigns [211]. However, the use of large-scale data analytics raises serious concerns about the privacy and security of sensitive customer data [212]. Although encryption and anonymization techniques [213] are used to protect data, challenges remain in ensuring that analytics processes do not expose personally identifiable information (PII) or sensitive transaction details. Research is needed into privacy-preserving data analytics techniques, such as federated learning, which allows for the analysis of data without exposing it to central servers. Additionally, research into the ethical implications of data analytics in e-commerce is necessary, as businesses must balance customer privacy with the need for data-driven insights.

5.9. Securing the supply chain

The security of the entire e-commerce supply chain is a growing concern [214], as vulnerabilities in one part of the chain can affect the entire ecosystem. Third-party suppliers, service providers, and logistics companies often have access to sensitive data, which can be exploited if not adequately secured [215], [216]. Research is needed to explore how to better secure the supply chain from cyberattacks, fraud, and data breaches, with a focus on developing security standards and best practices for third-party vendors. This research should include the creation of better tools for monitoring third-party risk, such as continuous risk assessments, and methods to ensure compliance with security protocols across the entire supply chain.

5.10. Privacy regulations and international compliance

As e-commerce platforms operate globally, complying with the diverse and constantly changing privacy regulations across different countries becomes increasingly difficult [217]. Existing research on data privacy laws often fails to address the complexities of cross-border data transfers and the enforcement of regulations in different legal systems [218]. Research gaps exist in developing solutions that enable businesses to achieve compliance with various regulations (such as GDPR, CCPA, and other regional privacy laws) while maintaining operational flexibility. There is also a need for more robust frameworks that support international data-sharing agreements without compromising privacy or security [219]. Research into automated compliance tools and cross-jurisdictional legal frameworks would help e-commerce businesses navigate these complex regulatory challenges.

As e-commerce platforms continue to grow and evolve, addressing these gaps is critical to staying ahead of emerging threats and ensuring robust protection of sensitive data. Researchers, businesses, and policymakers must collaborate to develop cutting-edge security solutions that meet the demands of modern e-commerce, balancing the need for strong protections with the user experience [220]. By addressing these challenges through targeted research and technological advancements, the e-commerce sector can continue to grow securely and sustainably in the face of evolving risks.

6. Future research directions

The future of e-commerce security and privacy is crucial for the continued growth and trust in online shopping and digital services. As e-commerce evolves with advancements in technology, so too must the methods used to secure online transactions, protect sensitive customer information, and maintain the privacy of individuals [221]. Future research in this area will need to address new challenges and opportunities posed by emerging technologies, new threat vectors, and the growing complexity of regulatory landscapes. The sub-sections below describe some of the future research directions in e-commerce security and privacy.

6.1. Artificial intelligence and machine learning for enhanced security

Artificial intelligence and machine learning have the potential to revolutionize e-commerce security by improving the detection of anomalies and identifying emerging threats [222], [223]. Future research should focus on developing more intelligent, adaptive, and accurate AI and ML-based security systems that can detect and mitigate new forms of attacks [224] in real time, including zero-day exploits, fraud, and advanced persistent threats. Current machine learning models in threat detection are often limited by high false-positive rates and inability to adapt quickly to novel attack strategies. Research should explore more advanced algorithms, such as deep learning and reinforcement learning, that can improve the system's ability to predict and respond to security incidents dynamically. Additionally, integrating AI-driven automated decision-making into e-commerce platforms could help provide faster and more efficient responses to cyber threats, reducing human intervention and response times.

6.2. Privacy-preserving technologies for data analytics

As privacy concerns rise, there is a pressing need for research into privacy-preserving technologies, particularly in the realm of data analytics [225]. E-commerce businesses rely heavily on data to optimize their services, personalize experiences, and drive marketing campaigns [226]. However, the collection, storage, and analysis of customer data pose significant privacy risks. Research should focus on technologies such as differential privacy, federated learning [227], and homomorphic encryption, which allow businesses to perform data analysis without exposing individual customer information. Additionally, future research should address the scalability and efficiency [228] of these technologies in the context of large-scale e-commerce platforms, where vast amounts of personal data are constantly being processed. A key focus should be developing privacy-preserving analytics that can handle complex datasets and provide actionable insights without compromising the privacy of users.

6.3. Blockchain and Distributed Ledger Technologies (DLT) for secure transactions

Blockchain and distributed ledger technologies hold promise for providing transparent, tamper-resistant, and secure transaction methods in e-commerce [229]. Blockchain's decentralized nature offers several advantages, such as reducing the reliance on intermediaries, enhancing data integrity, and preventing fraud [230]. Research should explore the broader application of blockchain in e-commerce beyond cryptocurrencies, particularly in areas such as smart contracts, decentralized identity management, and supply chain management. Future work can focus on addressing the challenges of blockchain scalability, energy efficiency, and latency, which currently hinder its widespread adoption [231], [232]. Additionally, integrating blockchain with existing e-commerce systems should be a focal point for researchers, ensuring seamless interoperability between blockchain networks and traditional payment systems or customer databases. The future of blockchain in e-commerce lies in its ability to create transparent, secure, and decentralized transactions, thereby enhancing user trust.

6.4. Advanced biometric authentication and behavior-based security

Traditional authentication methods, such as passwords and multi-factor authentication, are increasingly vulnerable to sophisticated attacks, including phishing, credential stuffing, and social engineering [233], [234]. One promising avenue for future research is behavioral biometrics, which uses unique behavioral patterns like typing speed, mouse movements, and navigation habits to authenticate users. Future research should aim to refine these methods to improve their accuracy, reliability, and user experience. Additionally, combining behavioral biometrics with multi-modal biometrics (e.g., face, voice, fingerprint recognition) [235] could create a more robust authentication system that is harder to bypass. Future studies should also explore the privacy implications of such biometric systems, ensuring that user data is protected and consented to in a transparent manner. Research into advanced biometric systems that are secure, user-friendly, and less intrusive could pave the way for more secure authentication methods for e-commerce platforms.

6.5. Quantum computing and cryptography

Quantum computing is on the horizon as a technology that promises to solve complex computational problems at a scale that is currently unattainable [236]. However, quantum computing also poses a serious threat to current encryption methods, such as RSA and ECC, which are commonly used to secure e-commerce transactions [237]. Future research in e-commerce security must focus on developing quantum-resistant cryptography that can withstand the power of quantum computers. This involves exploring new cryptographic algorithms [238] that are secure against quantum attacks and ensuring that these methods can be seamlessly integrated into e-commerce systems. Moreover, quantum key distribution (QKD) offers the potential to revolutionize secure communication in e-commerce by enabling ultra-secure methods of exchanging encryption keys [239]. As quantum computing technology advances, the research

community must ensure that the cryptographic systems used in e-commerce are adaptable and resilient to quantum-based threats.

6.6. Zero-trust security models for e-commerce

Zero-trust security is an emerging paradigm that assumes no entity, whether inside or outside the organization, should be trusted by default [240]. This security model is gaining traction in various industries, including e-commerce, as it offers a more robust way to protect sensitive data and systems in an increasingly interconnected world. Future research should focus on developing and refining zero-trust architectures for e-commerce platforms, where every transaction, user, and device is authenticated, authorized, and continuously monitored, regardless of its location. Research is needed to explore the integration of multi-factor authentication, micro-segmentation, continuous monitoring, and least privilege access into e-commerce systems [241] to create a comprehensive zero-trust environment. This model is particularly effective against insider threats, which remain a major concern in e-commerce security. Implementing zero-trust principles can help mitigate risks by ensuring that even if an attacker gains access to one part of the system, they cannot move laterally within the network.

6.7. Improved payment security methods

The security of online payment systems continues to be a critical concern for e-commerce businesses and consumers [242]. Future research should explore the development of more secure and efficient payment systems, particularly those that can prevent fraud and unauthorized transactions. Tokenization, which replaces sensitive payment information with a non-sensitive token, has already proven to be an effective solution [243], but more research is needed into how tokenization can be further optimized and integrated with emerging payment technologies, such as cryptocurrencies and digital wallets. Additionally, contactless payment security and peer-to-peer payment systems are gaining popularity, and research should focus on addressing the unique security challenges posed by these technologies. Ensuring seamless yet secure payment processes, along with robust fraud detection methods, will be essential to maintaining consumer trust in e-commerce platforms.

6.8. Privacy regulations and global compliance

As e-commerce continues to expand globally, it faces growing challenges related to data privacy regulations [244], which differ significantly across jurisdictions. Future research should focus on developing cross-border compliance frameworks that enable e-commerce platforms to meet the privacy and security requirements of various international markets. Understanding the implications of data localization laws, cross-border data transfers, and the varying requirements of General Data Protection Regulation, California Consumer Privacy Act, and other regional regulations is essential for e-commerce businesses operating in multiple regions. Research could also focus on the development of automated compliance tools that help businesses track and manage their obligations across multiple regulatory environments [245]. By making compliance processes more efficient, these tools would reduce the burden on e-commerce businesses and ensure they can maintain a high standard of privacy and security across all markets.

6.9. Cloud security and data protection

Cloud computing has become a cornerstone of modern e-commerce, offering scalability, flexibility, and cost savings [246]. However, it also introduces significant security and privacy challenges, particularly in areas like data storage, access control, and multi-cloud environments [247]. Future research should focus on improving cloud security architectures and developing innovative solutions for securing sensitive e-commerce data stored in the cloud. Topics for research include the development of end-to-end encryption, cloud access security brokers, and secure multi-party computation (SMPC) to protect data across cloud environments [248]. Moreover, research is needed on improving the security of cloud-based e-commerce services while maintaining the performance and efficiency [249] benefits that cloud computing offers. As businesses increasingly adopt hybrid and multi-cloud strategies, solutions must be found to ensure secure integration and management of cloud resources.

6.10. IoT security and privacy

The internet of things is transforming the e-commerce landscape by enabling connected devices that interact with online platforms, creating new opportunities for personalized experiences and smart services [250]. However, IoT devices introduce numerous security and privacy challenges, such as the risk of unauthorized access, data leakage, and device manipulation [251]-[253]. Future research should focus on securing IoT ecosystems, developing secure communication protocols for IoT devices, and implementing device authentication mechanisms that can protect against malicious attacks. Additionally, research is needed into ensuring the privacy of users' data when IoT devices collect and

transmit personal information [254], particularly in scenarios where IoT devices are integrated with e-commerce platforms for personalized marketing, smart home integration, or other customer services.

6.11. Ethical implications of e-commerce security

As e-commerce platforms collect vast amounts of personal data from users, there are growing concerns about the ethical implications of this data collection and use [255], [256]. Future research should focus on ethical guidelines for e-commerce security practices, addressing issues such as data minimization [257], consumer consent, and transparency in data usage. This includes exploring the ethical use of AI-driven recommendations, personalized marketing, and targeted advertising, ensuring that e-commerce businesses respect user privacy while still offering tailored services. Furthermore, the rise of dark patterns—design choices that manipulate users into making decisions that are not in their best interest—requires research into designing more ethical user interfaces and experiences that prioritize user privacy and security.

It is clear that the future of e-commerce security and privacy will be shaped by advances in technology, changing regulatory environments, and evolving threats. Researchers must address the gaps identified in AI, privacy-preserving technologies [258], blockchain, biometrics, and many other areas to develop solutions that can meet the demands of the modern e-commerce ecosystem. By staying ahead of emerging risks and leveraging new technologies, future research can help e-commerce businesses build secure, privacy-respecting systems that promote consumer trust and safeguard sensitive data [259]. Collaboration between academia, industry, and policymakers will be critical to creating a secure and sustainable e-commerce environment for the future.

7. Conclusion

This systematic review has examined the current state of data protection and privacy in the e-commerce environment, highlighting key challenges, solutions, and research gaps in safeguarding sensitive consumer information. As e-commerce continues to grow and evolve, the importance of robust data protection measures has become increasingly critical to maintain consumer trust and regulatory compliance. While a variety of technologies, including encryption, tokenization, and multi-factor authentication, have been implemented to enhance data security, privacy concerns remain a significant barrier to ensuring secure online transactions and protecting personal information from emerging threats. The review identified several key areas requiring further exploration, such as the development of privacy-preserving technologies like differential privacy and federated learning, the integration of blockchain for secure transactions, and the rise of behavioral biometrics for authentication. Additionally, the challenges posed by third-party vendors, insecure communication channels, and cross-border data transfers underline the need for more comprehensive security frameworks that address both technical and regulatory issues. Future research must focus on bridging these gaps by proposing scalable, adaptable, and user-centric solutions that balance security, privacy, and usability. By addressing these challenges and advancing security technologies, the e-commerce industry can enhance consumer confidence, ensure compliance with privacy regulations, and create a safer digital marketplace. Ultimately, a more secure and privacy-respecting e-commerce environment will be essential for fostering continued growth and innovation in the global digital economy.

References

[1] 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.

[2] Jain V, Malviya BI, Arya SA. An overview of electronic commerce (e-Commerce). The journal of contemporary issues in business and government. 2021 Jun 30;27(3):665-70.

[3] Guven H. Industry 4.0 and marketing 4.0: in perspective of digitalization and E-Commerce. InAgile Business Leadership Methods for Industry 4.0 2020 Oct 5 (pp. 25-46). Emerald Publishing Limited.

[4] Selvalakshmi B, Sudhakar G, Anbalagan A, Subashini K, Vijayalakshmi P, Kavin F. Enhancing E-Commerce Data Privacy in India's Rapidly Evolving Cybersecurity Landscape Through AI-Driven Intrusion Detection Systems. InStrategic Innovations of AI and ML for E-Commerce Data Security 2025 (pp. 261-280). IGI Global.

[5] Girimurugan B, Kumaresan V, Nair SG, Kuchi M, Kholifah N. AI and Machine Learning in E-Commerce Security: Emerging Trends and Practices. Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning. 2024:29-53.

[6] Abdali HK, Hussain MA, Abduljabbar ZA, Nyangaresi VO, Aldarwish AJ. Comprehensive Challenges to E-government in Iraq. InComputer Science On-line Conference 2024 Apr 25 (pp. 639-657). Cham: Springer Nature Switzerland.

[7] Morić Z, Dakic V, Djekic D, Regvart D. Protection of Personal Data in the Context of E-Commerce. Journal of cybersecurity and privacy. 2024 Sep 20;4(3):731-61.

[8] Rajendran R. Data Breach Fraudulence and Preventive Measures in E-Commerce Platforms. InAdvancements in Cybercrime Investigation and Digital Forensics 2024 (pp. 161-184). Apple Academic Press.

[9] Juneja A, Goswami S, Mondal S. Cyber security and digital economy: opportunities, growth and challenges. Journal of technology innovations and energy. 2024;3:1-22.

[10] Mannan MA. Data Privacy in E-Commerce: Challenges and Best Practices. InAnalyzing Privacy and Security Difficulties in Social Media: New Challenges and Solutions 2025 (pp. 415-440). IGI Global Scientific Publishing.

[11] Santoso B. Investigating Malware, Distributed Denial of Service Attacks, and Strategies for Data Protection in E-commerce. International Journal of Applied Business Intelligence. 2024 Dec 4;4(12):1-0.

[12] Nyangaresi VO, Alsolami E, Ahmad M. Trust-enabled Energy Efficient Protocol for Secure Remote Sensing in Supply Chain Management. IEEE Access. 2024 Aug 12.

[13] Martin KD, Kim JJ, Palmatier RW, Steinhoff L, Stewart DW, Walker BA, Wang Y, Weaven SK. Data privacy in retail. Journal of Retailing. 2020 Dec 1;96(4):474-89.

[14] 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.

[15] Bernovskis A, Sceulovs D, Stibe A. Society 5.0: Shaping the future of e-commerce. Journal of Open Innovation: Technology, Market, and Complexity. 2024 Dec 1;10(4):100391.

[16] Albshaier L, Almarri S, Hafizur Rahman MM. A review of blockchain's role in E-Commerce transactions: Open challenges, and future research directions. Computers. 2024 Jan 17;13(1):27.

[17] Jawad M, Yassin AA, AL-Asadi HA, Abduljabbar ZA, Nyangaresi VO. Towards Building Multi-factor Authentication Scheme for Users in the Healthcare Sector Based on Blockchain Technology. InComputer Science On-line Conference 2024 Apr 25 (pp. 694-713). Cham: Springer Nature Switzerland.

[18] Sureshkumar S, Thamilselvan R, Rani KU, Srinivasan V, Arularasan AN, Yuvasri B, Dadheech PD. E-Commerce Resilience Strategies for Mitigating 6G Security Threats. In6G Security Education and Multidisciplinary Implementation 2024 (pp. 154-171). IGI Global.

[19] Aragani VM, Maroju PK, Raju LN. Enhancing Cybersecurity in Banking: Best Practices and Solutions for Securing the Digital Supply Chain. Journal of Computational Analysis and Applications. 2024;33(8).

[20] Wang S, Asif M, Shahzad MF, Ashfaq M. Data privacy and cybersecurity challenges in the digital transformation of the banking sector. Computers & Security. 2024 Dec 1;147:104051.

[21] 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.

[22] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[23] Praveenadevi D, Velusamy C, Kumar S, Gogula R, Suryadevara S, Soans SV. Artificial Intelligence in E-Commerce: Protecting Data and Privacy. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 83-112). IGI Global.

[24] Karkuzhali K, Ravichandran MA, Rajeshwari S, Fufa G, Anujna N, Revanth P. Cloud Security for E-Commerce: Navigating Risks and Implementing Solutions. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 113-136). IGI Global.

[25] Kuchipudi R, Prathima T, Palamakula RB, Murthy TS, Rao KG. Private AI in E-Commerce: Safeguarding Consumer Data in the Digital Marketplace. InSustainable Development Using Private AI 2025 (pp. 232-239). CRC Press.

[26] Elluri L, Nagar A, Joshi KP. An integrated knowledge graph to automate gdpr and pci dss compliance. In2018 IEEE International Conference on Big Data (Big Data) 2018 Dec 10 (pp. 1266-1271). IEEE.

[27] Radhi BM, Hussain MA, Abduljabbar ZA, Nyangaresi VO, Aldarwish AJ. A Review on IoTs Applications and Security Threats via Data Transfer over Networks. InComputer Science On-line Conference 2024 Apr 25 (pp. 562-579). Cham: Springer Nature Switzerland.

[28] Adel A, Norouzifard M. Weaponization of the growing cybercrimes inside the dark net: The question of detection and application. Big Data and Cognitive Computing. 2024 Aug 14;8(8):91.

[29] 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.

[30] Singh B, Kaunert C, Singh G. Unraveling Financial Fraud With AI and Machine Learning: Screening Into Ad Clicks, Credit Card Management, and E-Commerce Transactions. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 406-429). IGI Global.

[31] Singh B, Kaunert C, Kaushik TK. Unscrambling Financial Fraud With AI and Machine Learning in E-Commerce Transactions: Airing Into Ad Clicks, Credit Card Management. InNavigating the Future of Finance in the Age of AI 2024 (pp. 253-271). IGI Global.

[32] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[33] Ayeni RK, Adebiyi AA, Okesola JO, Igbekele E. Phishing Attacks and Detection Techniques: A Systematic Review. In2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG) 2024 Apr 2 (pp. 1-17). IEEE.

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

[35] Zade S, Barhanpure S, Jaiswal SV, Kaur G, Agrawal P, Pinjarkar L. E-Commerce Cybersecurity: A Comprehensive Review of Types, Breaches and Best Practices. In2024 10th International Conference on Electrical Energy Systems (ICEES) 2024 Aug 22 (pp. 1-6). IEEE.

[36] Oroșanu MA, alexandru M. Cybercrime: A New Challenge of Criminality in the Digital Age. InInternational Conference on Cybersecurity and Cybercrime 2024 Nov 22 (Vol. 11, pp. 115-121).

[37] 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.

[38] Uddin MK, Rozony FZ, Kamruzzaman M. Common Cybersecurity Vulnerabilities: Software Bugs, Weak Passwords, Misconfigurations, Social Engineering. Social Engineering (August 20, 2024). 2024 Aug 20.

[39] Lestari S, Adawiyah WR, Alhamidi AL, Prayogi J, Haryanto R. Navigating perilous seas: unmasking online banking frauds, perceived usefulness, fear of cybercrime and distrust in online banking. Safer Communities. 2024 Sep 2;23(4):444-64.

[40] Rai R, Rohilla A, Rai A. Understanding Cybersecurity Threats in E-Commerce. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 501-522). IGI Global.

[41] Uddin R, Kumar SA, Chamola V. Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. Ad Hoc Networks. 2024 Jan 1;152:103322.

[42] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Aldarwish AJ, Neamah HA. Smart Grid and Renewable Energy Security Challenges: A Review. InComputer Science On-line Conference 2024 Apr 25 (pp. 805-825). Cham: Springer Nature Switzerland.

[43] Shivaji S. DDoS Attack Detection: Strategies, Techniques, and Future Directions. J. Electrical Systems. 2024;20(9s):2030-46.

[44] Perera S, Jin X, Maurushat A, Opoku DG. Factors affecting reputational damage to organisations due to cyberattacks. InInformatics 2022 Mar 18 (Vol. 9, No. 1, p. 28). MDPI.

[45] Patsakis C, Arroyo D, Casino F. The Malware as a Service ecosystem. InMalware: Handbook of Prevention and Detection 2024 Jul 5 (pp. 371-394). Cham: Springer Nature Switzerland.

[46] Singh SP, Afzal N. Effective Bot Management Strategies for Web Applications. In2024 International Symposium on Intelligent Robotics and Systems (ISoIRS) 2024 Jun 14 (pp. 314-322). IEEE.

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

[48] Butt UJ, Abbod MF, Kumar A. Cyber threat ransomware and marketing to networked consumers. InHandbook of research on innovations in technology and marketing for the connected consumer 2020 (pp. 155-185). IGI Global.

[49] Gupta R. Cybersecurity Threats in E-Commerce: Trends and Mitigation Strategies. Journal of Advanced Management Studies. 2024 Sep 7;1(3):1-0.

[50] Bhadouria AS. Study of: Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few of the World's Biggest Data Breaches. Int. J. Sci. Res. Publ. 2022.

[51] Nagar G. The evolution of ransomware: tactics, techniques, and mitigation strategies. International Journal of Scientific Research and Management (IJSRM). 2024 Jun;12(06):1282-98.

[52] Alshuraify NA, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Monitoring and surveillance systems based IoTs with Blockchain: Literature Review. Basrah Researches Sciences. 2024 Dec 31;50(2):42-63.

[53] George AS. When trust fails: Examining systemic risk in the digital economy from the 2024 crowdstrike outage. Partners Universal Multidisciplinary Research Journal. 2024 Jul 25;1(2):134-52.

[54] BN C, SH B. Revolutionizing ransomware detection and criticality assessment: multiclass hybrid machine learning and semantic similarity-based end2end solution. Multimedia Tools and Applications. 2024 Apr;83(13):39135-68.

[55] Ilca LF, Lucian OP, Balan TC. Enhancing cyber-resilience for small and medium-sized organizations with prescriptive malware analysis, detection and response. Sensors. 2023 Jul 28;23(15):6757.

[56] Wang X, Yan Z, Zhang R, Zhang P. Attacks and defenses in user authentication systems: A survey. Journal of Network and Computer Applications. 2021 Aug 15;188:103080.

[57] 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.

[58] Badotra S, Sundas A. A systematic review on security of E-commerce systems. International Journal of Applied Science and Engineering. 2021 Jun;18(2):1-9.

[59] ALGhamdi SA, Daim T, Meissner D. Electronic payment technology: Developing a taxonomy of factors to evaluate a fraud detection and prevention system for the airlines industry. InThe Routledge Companion to Technology Management 2022 Aug 31 (pp. 450-511). Routledge.

[60] Patil S, Dudhankar V, Shukla P. Enhancing Digital Security: How Identity Verification Mitigates E-Commerce Fraud. Journal of Current Science and Research Review. 2024 Dec 13;2(02):69-81.

[61] Zaini SM, Noor NH, Zandi G. The behaviour of e-commerce users: An empirical investigation of online shopping. Journal of Management World. 2024;2024(2):50-60.

[62] Abdali HK, Hussain MA, Abduljabbar ZA, Nyangaresi VO. Implementing Blockchain for Enhancing Security and Authentication in Iraqi E-Government Services. Engineering, Technology & Applied Science Research. 2024 Dec 2;14(6):18222-33.

[63] Dragomirov N. E-commerce platforms and supply chain management–functionalities study. Economic Alternatives. 2020;2:250-61.

[64] Ali SA. Designing Secure and Robust E-Commerce Plaform for Public Cloud. The Asian Bulletin of Big Data Management. 2023 Nov 25;3(1):164-89.

[65] Urrea NT, Vishkaei BM, De Giovanni P. Operational Risk Management in E-Commerce: A Platform Perspective. IEEE Transactions on Engineering Management. 2024 Jan 29.

[66] Rajendran RK. Data Privacy and Security Risks in Third-Party App Integrations. InAnalyzing Privacy and Security Difficulties in Social Media: New Challenges and Solutions 2025 (pp. 311-334). IGI Global Scientific Publishing.

[67] 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.

[68] Searle R, Renaud KV, van der Werff L. Shaken to the core: trust trajectories in the aftermaths of adverse cyber events. Journal of Intellectual Capital. 2024 Nov 8;25(5/6):1154-83.

[69] Kampourakis V, Kambourakis G, Chatzoglou E, Zaroliagis C. Revisiting man-in-the-middle attacks against HTTPS. Network Security. 2022 Mar;2022(3).

[70] 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.

[71] Maheshwaran T, Muthumarilakshmi S, Vinoth NA, Suganya K, Maheswari B, Girija P. Securing E-Commerce Strategies With Cloud, Blockchain, AI, and ML. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 470-500). IGI Global.

[72] Al-Maliki H, AL-Asadi HA, Abduljabbar ZA, Nyangaresi VO. Reliable Vehicular Ad Hoc Networks for Intelligent Transportation Systems based on the Snake Optimization Algorithm. Engineering, Technology & Applied Science Research. 2024 Dec 2;14(6):18631-9.

[73] Elshoush HT, Mohammed RM, Abdelhameed MT, Mohammed AF. Mitigating Man-in-the-middle Attack In Online Payment System Transaction Using Polymorphic AES Encryption Algorithm. J. Inf. Hiding Multim. Signal Process.. 2023 Sep;14(3):102-12.

[74] Nookala G. The Role of SSL/TLS in Securing API Communications: Strategies for Effective Implementation. Journal of Computing and Information Technology. 2024 Feb 13;4(1).

[75] Hummer D, Rebovich DJ. Identity theft and financial loss. InHandbook on Crime and Technology 2023 Mar 28 (pp. 38-53). Edward Elgar Publishing.

[76] Spanca F, Salihu A. Unveiling the Consequences of Data Breaches: Risks, Impacts, and Mitigation in the Digital Age. In2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE) 2024 Oct 30 (pp. 1-8). IEEE.

[77] 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.

[78] Ogundele IO, Akinade AO, Alakiri HO, Aromolaran AA, Uzoma BO. Detection and prevention of session hijacking in web application management. Int J Adv Res Comput Commun Eng. 2020 Jul;9(6):1-0.

[79] Drakonakis K, Ioannidis S, Polakis J. The cookie hunter: Automated black-box auditing for web authentication and authorization flaws. InProceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security 2020 Oct 30 (pp. 1953-1970).

[80] Calzavara S, Jonker H, Krumnow B, Rabitti A. Measuring web session security at scale. Computers & Security. 2021 Dec 1;111:102472.

[81] Mallick MA, Nath R. Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. World Scientific News. 2024;190(1):1-69.

[82] Radhi BM, Hussain MA, Abduljabbar ZA, Nyangaresi VO. Secure and Fast Remote Application–Based Authentication Dragonfly Using an LED Algorithm in Smart Buildings. In2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2024 Feb 19 (pp. 509-517). IEEE.

[83] Praveenadevi D, Saxena M, Suganya T, Bhavana M, Yadav BN, Wakuma L. Harnessing Cloud Technologies for Secure E-Commerce. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 310-332). IGI Global.

[84] Hazra R, Chatterjee P, Singh Y, Podder G, Das T. Data Encryption and Secure Communication Protocols. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 546-570). IGI Global.

[85] Lakshmi BS, Kovvuri D, Bolisetti HV, Chikkala DS, Karri S, Yadlapalli G. A proactive approach for detecting SQL and XSS injection attacks. In2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) 2024 Jun 5 (pp. 1415-1420). IEEE.

[86] Borana GK, Vishwakarma NH, Tamboli S, Sharma P, Mukhedkar MM, Dawande NA. Defending the Digital World: A Comprehensive Guide Against SQL Injection Threats. In2024 Second International Conference on Inventive Computing and Informatics (ICICI) 2024 Jun 11 (pp. 707-714). IEEE.

[87] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[88] Paul A, Sharma V, Olukoya O. SQL injection attack: Detection, prioritization & prevention. Journal of Information Security and Applications. 2024 Sep 1;85:103871.

[89] Thilakraj M, Anupriya S, Cibi MM, Divya A. Detection of SQL Injection Attacks. In2024 International Conference on Inventive Computation Technologies (ICICT) 2024 Apr 24 (pp. 1515-1520). IEEE.

[90] Nair SS. Securing Against Advanced Cyber Threats: A Comprehensive Guide to Phishing, XSS, and SQL Injection Defense. Journal of Computer Science and Technology Studies. 2024 Jan 14;6(1):76-93.

[91] Samo A, Halepoto MA, Awan K, Jinjhin JA, Shaikh M, Arain QA. An In-Depth Analysis of Cross-site Scripting (XSS): Threats, Mechanisms, and Mitigation Strategies. Organized by: The Benazir Bhutto Shaheed University of Technology and Skill Development, Khairpur Mirs. 2024;2024(2nd):122.

[92] Alzaidi ZS, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Development Anonymous Authentication Maria et al.'s Scheme of VANETs Using Blockchain and Fog Computing with QR Code Technique. In2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) 2024 Jul 1 (pp. 2247-2252). IEEE.

[93] Chowdhury MA, Rahman M, Rahman S. Detecting vulnerabilities in website using multiscale approaches: based on case study. International Journal of Electrical & Computer Engineering (2088-8708). 2024 Jun 1;14(3).

[94] Saxena N, Hayes E, Bertino E, Ojo P, Choo KK, Burnap P. Impact and key challenges of insider threats on organizations and critical businesses. Electronics. 2020 Sep 7;9(9):1460.

[95] Al-Harrasi A, Shaikh AK, Al-Badi A. Towards protecting organisations' data by preventing data theft by malicious insiders. International Journal of Organizational Analysis. 2023 Apr 10;31(3):875-88.

[96] Pandey S, Singh RK, Gunasekaran A, Kaushik A. Cyber security risks in globalized supply chains: conceptual framework. Journal of Global Operations and Strategic Sourcing. 2020 Feb 10;13(1):103-28.

[97] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[98] 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.

[99] Praveenadevi D, Sathyasundari S, Dakshinamurthy T, Syamala M, Gundapaneni M, Pattnaik M. Cybersecurity Strategies for E-Commerce: Best Practices and Case Studies. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 137-158). IGI Global.

[100] Ma X, Wang Z. Computer security technology in E-commerce platform business model construction. Heliyon. 2024 Apr 15;10(7).

[101] Nookala G, Gade KR, Dulam N, Thumburu SK. SSL Pinning: Strengthening SSL Security for Mobile Applications. Innovative Engineering Sciences Journal. 2024 Nov 18;4(1).

[102] Jawad M, Yassin AA, Al-Asadi HA, Abduljabbar ZA, Nyangaresi VO. IoHT System Authentication Through the Blockchain Technology: A Review. In2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) 2024 Jul 1 (pp. 2253-2258). IEEE.

[103] D'Orazio CJ, Choo KK. A technique to circumvent SSL/TLS validations on iOS devices. Future Generation Computer Systems. 2017 Sep 1; 74:366-74.

[104] Nookala G, Gade KR, Dulam N, Thumburu SK. End-to-End Encryption in Enterprise Data Systems: Trends and Implementation Challenges. Innovative Computer Sciences Journal. 2019 Sep 18;5(1).

[105] Swanzy PN, Abukari AM, Ansong ED. Data Security Framework for Protecting Data in Transit and Data at Rest in the Cloud. Current Journal of Applied Science and Technology. 2024 May 13;43(6):61-77.

[106] Aburbeian AM, Fernández-Veiga M. Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning. AI. 2024 Jan 10;5(1):177-94.

[107] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[108] Kamaruddin NH, Zolkipli MF. The Role of Multi-Factor Authentication in Mitigating Cyber Threats. Borneo International Journal eISSN 2636-9826. 2024 Dec 16;7(4):35-42.

[109] Patil S, Dudhankar V, Shukla P. Securing Digital Transactions: The Role of Identity Verification in Reducing E-Commerce Fraud. Journal of Artificial Intelligence Research. 2023 Jun 23;3(1):358-85.

[110] Yıldırım M, Mackie I. Encouraging users to improve password security and memorability. International Journal of Information Security. 2019 Dec; 18:741-59.

[111] Shammee TI, Akter T, Mou M, Chowdhury F, Ferdous MS. A systematic literature review of graphical password schemes. Journal of Computing Science and Engineering. 2020 Dec;14(4):163-85.

[112] Alshuraify NA, Yassin AA, Abduljabbar ZA, Nyangaresi VO, Aldarwish AJ. Blockchain-Based CCTV Surveillance Cameras for Oil and Gas Industry Pipelines. InComputer Science On-line Conference 2024 Apr 25 (pp. 730-744). Cham: Springer Nature Switzerland.

[113] Gayam SR. AI-Driven Fraud Detection in E-Commerce: Advanced Techniques for Anomaly Detection, Transaction Monitoring, and Risk Mitigation. Distributed Learning and Broad Applications in Scientific Research. 2020 Nov 25; 6:124-51.

[114] Khurana R. Fraud detection in ecommerce payment systems: The role of predictive ai in real-time transaction security and risk management. International Journal of Applied Machine Learning and Computational Intelligence. 2020;10(6):1-32.

[115] Chatterjee P, Das D, Rawat DB. Digital twin for credit card fraud detection: Opportunities, challenges, and fraud detection advancements. Future Generation Computer Systems. 2024 Apr 30.

[116] Welekar R, Ismail FS, Bhojwani A, Mehar S, Tidke P, Bopche P. Web application firewall. InAIP Conference Proceedings 2024 Nov 4 (Vol. 3214, No. 1). AIP Publishing.

[117] 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.

[118] Kamruzzaman A, Ismat S, Brickley JC, Liu A, Thakur K. A comprehensive review of endpoint security: Threats and defenses. In2022 International Conference on Cyber Warfare and Security (ICCWS) 2022 Dec 7 (pp. 1-7). IEEE.

[119] Vasani V, Bairwa AK, Joshi S, Pljonkin A, Kaur M, Amoon M. Comprehensive analysis of advanced techniques and vital tools for detecting malware intrusion. Electronics. 2023 Oct 17;12(20):4299.

[120] Jayalath RK, Ahmad H, Goel D, Syed MS, Ullah F. Microservice vulnerability analysis: A literature review with empirical insights. IEEE Access. 2024 Oct 16.

[121] Rahaman M, Bakkireddygari SS, Chattopadhyay S, Gomez AL, Arya V, Bansal S. Infrastructure and Network Security. InMetaverse Security Paradigms 2024 (pp. 108-144). IGI Global.

[122] Alshuraify A, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Blockchain-based Authentication Scheme in Oil and Gas Industry Data with Thermal CCTV Cameras Applications to Mitigate Sybil and 51% Cyber Attacks. International Journal of Intelligent Engineering & Systems. 2024 Nov 1;17(6).

[123] Sathiyapriyan C, Manikandan B, Gokul S, Satheesh R, Nivetha S, Leelavathy S. Strategies for Building and Maintaining Secure Web Applications. In2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI) 2024 Jan 18 (pp. 803-809). IEEE.

[124] Wodi A. The EU General Data Protection Regulation (GDPR): Five Years After and the Future of Data Privacy Protection in Review. GDPR: Five Years After and the Future of Data Privacy Protection in Review (July-Oct. 2023). 2023.

[125] Tran VH, Mehrotra A, Chetty M, Feamster N, Frankenreiter J, Strahilevitz L. Measuring Compliance with the California Consumer Privacy Act Over Space and Time. InProceedings of the CHI Conference on Human Factors in Computing Systems 2024 May 11 (pp. 1-19).

[126] Samira Z, Weldegeorgise YW, Osundare OS, Ekpobimi HO, Kandekere RC. Comprehensive data security and compliance framework for SMEs. Magna Scientia Advanced Research and Reviews. 2024;12(1):043-55.

[127] 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.

[128] Belghith A. e-CommerceShield: A Framework for Enhanced Security in E-Commerce with Awareness, DNS Matching, and Blockchain Integration. In2024 IEEE 30th International Conference on Telecommunications (ICT) 2024 Jun 24 (pp. 01-06). IEEE.

[129] Kollar AM, Katona J. Enhancing Password Security: Analyzing Password Management Practices Among IT Students. In2024 IEEE 7th International Conference and Workshop Óbuda on Electrical and Power Engineering (CANDO-EPE) 2024 Oct 17 (pp. 000059-000064). IEEE.

[130] Houcheimi A, Mezei J. The Role of Secure Online Payments in Enabling the Development of E-Tailing. Journal of Organizational Computing and Electronic Commerce. 2024 Oct 1;34(4):299-317.

[131] Shabina, Ali RF, Jahankhani H, Siddiqi Y, Hassan B. Ensuring Securing PII Data in the AWS Cloud: A Comprehensive Guide to PCI DSS Compliance. InCybersecurity and Artificial Intelligence: Transformational Strategies and Disruptive Innovation 2024 Apr 18 (pp. 185-216). Cham: Springer Nature Switzerland.

[132] Duaa Fadhel Najem, Nagham Abdulrasool Taha, Zaid Ameen Abduljabbar, Vincent Omollo Nyangaresi, Junchao Ma and Dhafer G. Honi. Low-Complexity and Secure Clustering-Based Similarity Detection for Private Files. TEM Journal, 13(2), 2341-2349 (2024).

[133] Park H, Huo Y, Yoon SE. Meshchain: Secure 3d model and intellectual property management powered by blockchain technology. InAdvances in Computer Graphics: 38th Computer Graphics International Conference, CGI 2021, Virtual Event, September 6–10, 2021, Proceedings 38 2021 (pp. 519-534). Springer International Publishing.

[134] Fauziyah F, Wang Z, Joy G. Knowledge Management Strategy for Handling Cyber Attacks in E-Commerce with Computer Security Incident Response Team (CSIRT). Journal of Information Security. 2022 Aug 23;13(4):294-311.

[135] Sreekala SP, Rajnarayanan B, Gokul K, Bommasani K, Harini GN, Fufa G. Leadership in E-Commerce Security: Managing Risks and Innovations. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 254-276). IGI Global.

[136] Tatineni S. Cloud-Based Business Continuity and Disaster Recovery Strategies. International Research Journal of Modernization in Engineering, Technology, and Science. 2023 Nov;5(11):1389-97.

[137] 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.

[138] Gupta A, Yadav H, Sharma S. Revolutionizing E-Commerce Security: A Secured Infrastructure Utilizing BlockChain. In2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) 2024 Jun 24 (pp. 1-6). IEEE.

[139] Liu X, Ahmad SF, Anser MK, Ke J, Irshad M, Ul-Haq J, Abbas S. Cyber security threats: A never-ending challenge for e-commerce. Frontiers in psychology. 2022 Oct 19;13:927398.

[140] Barta J, Nyikes Z. Cyber Threats to Consumers and Other Risks in the Field of E-commerce Security. InIFIP International Conference on Human Choice and Computers 2022 Sep 8 (pp. 33-43). Cham: Springer Nature Switzerland.

[141] Mustapha AA, Udeh AS, Ashi TA, Sobowale OS, Akinwande MJ, Oteniara AO. Comprehensive review of machine learning models for sql injection detection in e-commerce. World Journal of Advanced Research and Reviews. 2024;23(1):451-65.

[142] Al Sibahee MA, Abduljabbar ZA, Ngueilbaye A, Luo C, Li J, Huang Y, Zhang J, Khan N, Nyangaresi VO, Ali AH. Blockchain-Based Authentication Schemes in Smart Environments: A Systematic Literature Review. IEEE Internet of Things Journal. 2024 Jul 3.

[143] 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.

[144] Guembe B, Azeta A, Misra S, Osamor VC, Fernandez-Sanz L, Pospelova V. The emerging threat of ai-driven cyber attacks: A review. Applied Artificial Intelligence. 2022 Dec 31;36(1):2037254.

[145] Kusuma P. A Holistic Framework for Designing Secure, Scalable, and Cost-Effective Cloud-Based E-Commerce Platforms. Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures. 2022 Dec 7;6(12):7-16.

[146] Khanna A. Case Studies in the E-commerce Industry. InSecuring an Enterprise: Maximizing Digital Experiences through Enhanced Security Measures 2025 Jan 1 (pp. 307-327). Berkeley, CA: Apress.

[147] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

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

[149] Rodrigues VF, Policarpo LM, da Silveira DE, da Rosa Righi R, da Costa CA, Barbosa JL, Antunes RS, Scorsatto R, Arcot T. Fraud detection and prevention in e-commerce: A systematic literature review. Electronic Commerce Research and Applications. 2022 Nov 1;56:101207.

[150] Ataullah M, Chauhan N. Exploring security and privacy enhancement technologies in the Internet of Things: A comprehensive review. Security and Privacy. 2024 Nov;7(6):e448.

[151] Thabit F, Can O, Aljahdali AO, Al-Gaphari GH, Alkhzaimi HA. Cryptography algorithms for enhancing IoT security. Internet of Things. 2023 Jul 1;22:100759.

[152] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Abduljaleel IQ, Aldarwish AJ. A Provably Secure Anonymous Authentication Protocol for Consumer and Service Provider Information Transmissions in Smart Grids. Cryptography. 2024 May 9;8(2):20.

[153] Lu F. Online shopping consumer perception analysis and future network security service technology using logistic regression model. PeerJ Computer Science. 2024 Jan 15;10:e1777.

[154] Az-zahra A, Cahyani ND, Suryani V. Analysis of User Personal Data Security at E-Commerce Based on User Viewpoints. In2024 12th International Conference on Information and Communication Technology (ICoICT) 2024 Aug 7 (pp. 86-92). IEEE.

[155] Kheruddin MS, Zuber MA, Radzai MM. Phishing Attacks: Unraveling Tactics, Threats, and Defenses in the Cybersecurity Landscape. Authorea Preprints. 2024 Jan 15.

[156] Jøsang A. Attack Vectors and Malware. InCybersecurity: Technology and Governance 2024 Nov 29 (pp. 25-42). Cham: Springer Nature Switzerland.

[157] 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.

[158] Rehman F, Mushtaq F, Zaman H. A Host-based Intrusion Detection: Using Signature-based and AI-driven Anomaly Detection for Enhanced Cybersecurity. In2024 4th International Conference on Digital Futures and Transformative Technologies (ICoDT2) 2024 Oct 22 (pp. 1-7). IEEE.

[159] Arun A, Nair AS, Sreedevi AG. Zero Day Attack Detection and Simulation through Deep Learning Techniques. In2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence) 2024 Jan 18 (pp. 852-857). IEEE.

[160] Adeniran IA, Efunniyi CP, Osundare OS, Abhulimen AO. Enhancing security and risk management with predictive analytics: A proactive approach. International Journal of Management & Entrepreneurship Research. 2024;6(8).

[161] Ilić L, Šijan A, Predić B, Viduka D, Karabašević D. Research Trends in Artificial Intelligence and Security—Bibliometric Analysis. Electronics. 2024 Jan;13(12):2288.

[162] Ali AH, Jasim HM, Abduljabbar ZA, Nyangaresi VO, Umran SM, Ma J, Honi DG. Provably Efficient and Fast Technique for Determining the Size of a Brain Tumor in T1 MRI Images. In2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2024 Feb 19 (pp. 608-613). IEEE.

[163] Lazić A, Milić S, Vukmirović D. The Future of Electronic Commerce in the IoT Environment. Journal of Theoretical and Applied Electronic Commerce Research. 2024 Jan 24;19(1):172-87.

[164] Weichbroth P, Łysik Ł. Mobile security: Threats and best practices. Mobile Information Systems. 2020;2020(1):8828078.

[165] Rus AC, El-Hajj M, Sarmah DK. NAISS: A reverse proxy approach to mitigate MageCart's e-skimmers in e-commerce. Computers & Security. 2024 May 1;140:103797.

[166] Ullah I, Adhikari D, Ali F, Ali A, Khan H, Sharafian A, Kesavan SM, Bai X. Revolutionizing E-Commerce With Consumer-Driven Energy-Efficient WSNs: A Multi-Characteristics Approach. IEEE Transactions on Consumer Electronics. 2024 Jun 10.

[167] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[168] Farhad MA. Consumer data protection laws and their impact on business models in the tech industry. Telecommunications Policy. 2024 Oct 1;48(9):102836.

[169] Chinamanagonda S. Automating Cloud Governance-Organizations automating compliance and governance in the cloud. MZ Computing Journal. 2021 May 11;2(1).

[170] Gal MS, Aviv O. The competitive effects of the GDPR. Journal of Competition Law & Economics. 2020 Sep;16(3):349-91.

[171] Salamkar MA. Scalable Data Architectures: Key principles for building systems that efficiently manage growing data volumes and complexity. Journal of AI-Assisted Scientific Discovery. 2021 Jan 6;1(1):251-70.

[172] Bulbul SS, Abduljabbar ZA, Mohammed RJ, Al Sibahee MA, Ma J, Nyangaresi VO, Abduljaleel IQ. A provably lightweight and secure DSSE scheme, with a constant storage cost for a smart device client. Plos one. 2024 Apr 25;19(4):e0301277.

[173] Akindote O, Enyejo JO, Awotiwon BO, Ajayi AA. Integrating Blockchain and Homomorphic Encryption to Enhance Security and Privacy in Project Management and Combat Counterfeit Goods in Global Supply Chain Operations. International Journal of Innovative Science and Research Technology. 2024 Nov;9(11).

[174] Ahmad W, Rasool A, Javed AR, Baker T, Jalil Z. Cyber security in iot-based cloud computing: A comprehensive survey. Electronics. 2021 Dec 22;11(1):16.

[175] Badwan N. Role of supply chain partnership, cross-functional integration, responsiveness and resilience on competitive advantages: empirical evidence from Palestine. The TQM Journal. 2024 May 17.

[176] Syed NF, Shah SW, Trujillo-Rasua R, Doss R. Traceability in supply chains: A Cyber security analysis. Computers & Security. 2022 Jan 1;112:102536.

[177] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[178] Li W, Xiao JX, Zhang MT. Optimizing Urban e-Commerce Experiences: A Cross-Cultural Interface Design Approach for Enhanced Connectivity and Consumer Engagement. InInternational Conference on Human-Computer Interaction 2024 Jun 1 (pp. 219-234). Cham: Springer Nature Switzerland.

[179] Otta SP, Panda S, Gupta M, Hota C. A systematic survey of multi-factor authentication for cloud infrastructure. Future Internet. 2023 Apr 10;15(4):146.

[180] Fathima AR, Saravanan A. An approach to cloud user access control using behavioral biometric-based authentication and continuous monitoring. International Journal of Advanced Technology and Engineering Exploration. 2024 Oct 1;11(119):1469.

[181] Rachamim M, Hornik J, Ofir C. The market for private security: a review, research agenda, and marketing strategies for a contested terrain. Management Review Quarterly. 2023 Oct 4:1-41.

[182] Al Sibahee MA, Abduljabbar ZA, Luo C, Zhang J, Huang Y, Abduljaleel IQ, Ma J, Nyangaresi VO. Hiding scrambled text messages in speech signals using a lightweight hyperchaotic map and conditional LSB mechanism. Plos one. 2024 Jan 3;19(1):e0296469.

[183] Baako I, Umar S. An integrated vulnerability assessment of electronic commerce websites. International Journal of Information Engineering and Electronic Business. 2020 Oct 1;14(5):24.

[184] Olateju O, Okon SU, Igwenagu U, Salami AA, Oladoyinbo TO, Olaniyi OO. Combating the challenges of false positives in AI-driven anomaly detection systems and enhancing data security in the cloud. Available at SSRN 4859958. 2024 Jun 10.

[185] Sharma A, Kumar VG, Poojari A. Prioritize Threat Alerts Based on False Positives Qualifiers Provided by Multiple AI Models Using Evolutionary Computation and Reinforcement Learning. Journal of The Institution of Engineers (India): Series B. 2024 Oct 29:1-8.

[186] Bécue A, Praça I, Gama J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review. 2021 Jun;54(5):3849-86.

[187] 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.

[188] Manda JK. Privacy-Preserving Technologies in Telecom Data Analytics: Implementing Privacy-Preserving Techniques Like Differential Privacy to Protect Sensitive Customer Data During Telecom Data Analytics. MZ Computing Journal. 2023 May 25;4(1).

[189] Farayola OA, Olorunfemi OL, Shoetan PO. Data privacy and security in it: a review of techniques and challenges. Computer Science & IT Research Journal. 2024 Mar 27;5(3):606-15.

[190] Thantharate P, Bhojwani S, Thantharate A. DPShield: Optimizing Differential Privacy for High-Utility Data Analysis in Sensitive Domains. Electronics. 2024 Jun 14;13(12):2333.

[191] Dhavamani L, Ananthavadivel D, Akilandeswari P, Nanajappan M. Differential Privacy-Preserving IoT Data Sharing Through Enhanced PSO. Journal of Computer Information Systems. 2024 Jul 8:1-7.

[192] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA. Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. Plos one. 2024 Jan 23;19(1):e0296781.

[193] Khadka M. A Systematic Appraisal of Multi-Factor Authentication Mechanisms for Cloud-Based E-Commerce Platforms and Their Effect on Data Protection. Journal of Emerging Cloud Technologies and Cross-Platform Integration Paradigms. 2022 Dec 7;6(12):12-21.

[194] Arshad R, Asghar MR. Characterisation and quantification of user privacy: key challenges, regulations, and future directions. IEEE Communications Surveys & Tutorials. 2024 Dec 18.

[195] Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security. 2017 Jan 1;64:122-34.

[196] Esteves B, Pandit HJ, Rodríguez-Doncel V. ODRL profile for expressing consent through granular access control policies in solid. In2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) 2021 Sep 6 (pp. 298-306). IEEE.

[197] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[198] Habib G, Sharma S, Ibrahim S, Ahmad I, Qureshi S, Ishfaq M. Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet. 2022 Nov 21;14(11):341.

[199] Chen Y, Bellavitis C. Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights. 2020 Jun 1;13:e00151.

[200] Menard P, Bott GJ. Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. Computers & Security. 2020 Aug 1;95:101856.

[201] Omolara AE, Alabdulatif A, Abiodun OI, Alawida M, Alabdulatif A, Arshad H. The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security. 2022 Jan 1;112:102494.

[202] 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.

[203] Jandl C, Wagner M, Moser T, Schlund S. Reasons and strategies for privacy features in tracking and tracing systems—a systematic literature review. Sensors. 2021 Jun 30;21(13):4501.

[204] Asante M, Epiphaniou G, Maple C, Al-Khateeb H, Bottarelli M, Ghafoor KZ. Distributed ledger technologies in supply chain security management: A comprehensive survey. IEEE Transactions on Engineering Management. 2021 Mar 1;70(2):713-39.

[205] Benčić FM, Skočir P, Žarko IP. DL-Tags: DLT and smart tags for decentralized, privacy-preserving, and verifiable supply chain management. IEEE access. 2019 Apr 9;7:46198-209.

[206] Mohammed Abdul SS. Navigating blockchain's twin challenges: Scalability and regulatory compliance. Blockchains. 2024 Jul 21;2(3):265-98.

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

[208] Pureti N. Implementing Multi-Factor Authentication (MFA) to Enhance Security. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 2020 Sep 2;11(1):15-29.

[209] Hlongwane TC, Mathonsi TE, Du Plessis D, Muchenje T. A Survey of Biometric Recognition Systems in E-Business Transactions. International Journal of Communication Networks and Information Security. 2023 Dec 1;15(4):263-79.

[210] Ioannou A, Tussyadiah I, Lu Y. Privacy concerns and disclosure of biometric and behavioral data for travel. International Journal of Information Management. 2020 Oct 1;54:102122.

[211] Akshara R, Jain A. Data to Decisions: Optimizing E-commerce Sales Potential with Analytics. International Research Journal on Advanced Engineering Hub (IRJAEH). 2024 Apr 27;2(04):1087-93.

[212] Wieringa J, Kannan PK, Ma X, Reutterer T, Risselada H, Skiera B. Data analytics in a privacy-concerned world. Journal of Business Research. 2021 Jan 1;122:915-25.

[213] Yenurkar G, Mal S, Nyangaresi VO, Kamble S, Damahe L, Bankar N. Revolutionizing Chronic Heart Disease Management: The Role of IoT-Based Ambulatory Blood Pressure Monitoring System. Diagnostics. 2024 Jun 19;14(12):1297.

[214] Zawaideh FH, Abu-ulbeh W, Majdalawi YI, Zakaria MD, Jusoh JA, Das S. E-Commerce Supply Chains with Considerations of Cyber-Security. In2023 International Conference on Computer Science and Emerging Technologies (CSET) 2023 Oct 10 (pp. 1-8). IEEE.

[215] Shaverdian P. Start with trust: Utilizing blockchain to resolve the third-party data breach problem. UCLA L. Rev.. 2019;66:1242.

[216] Odimarha AC, Ayodeji SA, Abaku EA. Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies. World Journal of Advanced Science and Technology. 2024;5(1):026-30.

[217] Choraś M, Pawlicka A, Jaroszewska-Choraś D, Pawlicki M. Not Only Security and Privacy: The Evolving Ethical and Legal Challenges of E-Commerce. InEuropean Symposium on Research in Computer Security 2023 Sep 25 (pp. 167-181). Cham: Springer Nature Switzerland.

[218] Tehrani PM, Sabaruddin JS, Ramanathan DA. Cross border data transfer: Complexity of adequate protection and its exceptions. Computer law & security review. 2018 Jun 1;34(3):582-94.

[219] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[220] Okoli K, Bekeneva Y. Balancing security and user experience in the evolving digital landscape. InE3S Web of Conferences 2024 (Vol. 471, p. 04007). EDP Sciences.

[221] Bandara R, Fernando M, Akter S. Privacy concerns in E-commerce: A taxonomy and a future research agenda. Electronic Markets. 2020 Sep;30(3):629-47.

[222] Karunaratne T. Machine Learning and Big Data Approaches to Enhancing E-commerce Anomaly Detection and Proactive Defense Strategies in Cybersecurity. Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures. 2023 Dec 4;7(12):1-6.

[223] Mudgal A. Leveraging AI and ML for Proactive Threat Detection for E-Commerce. InStrategic Innovations of AI and ML for E-Commerce Data Security 2025 (pp. 281-322). IGI Global.

[224] 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.

[225] Yu S, Carroll F, Bentley BL. Insights Into Privacy Protection Research in AI. IEEE Access. 2024 Mar 18;12:41704-26.

[226] Raji MA, Olodo HB, Oke TT, Addy WA, Ofodile OC, Oyewole AT. E-commerce and consumer behavior: A review of AI-powered personalization and market trends. GSC Advanced Research and Reviews. 2024;18(3):066-77.

[227] Li J, Cui T, Yang K, Yuan R, He L, Li M. Demand forecasting of e-commerce enterprises based on horizontal federated learning from the perspective of sustainable development. Sustainability. 2021 Nov 25;13(23):13050.

[228] 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).

[229] Agarwal U, Rishiwal V, Tanwar S, Chaudhary R, Sharma G, Bokoro PN, Sharma R. Blockchain technology for secure supply chain management: A comprehensive review. Ieee Access. 2022 Jul 27;10:85493-517.

[230] Mustyala A. Leveraging Blockchain for Fraud Risk Reduction in Fintech: Infrastructure Setup and Migration Strategies. EPH-International Journal of Science And Engineering. 2023 Apr 12;9(2):1-0.

[231] Khan D, Jung LT, Hashmani MA. Systematic literature review of challenges in blockchain scalability. Applied Sciences. 2021 Oct 9;11(20):9372.

[232] Sanka AI, Cheung RC. A systematic review of blockchain scalability: Issues, solutions, analysis and future research. Journal of Network and Computer Applications. 2021 Dec 1;195:103232.

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

[234] Konidala S. Understanding the different types of authentication methods. Australian Journal of Machine Learning Research & Applications. 2022 Nov 6;2(2):385-406.

[235] Pahuja S, Goel N. Multimodal biometric authentication: A review. AI Communications. 2024(Preprint):1-23.

[236] Memon QA, Al Ahmad M, Pecht M. Quantum Computing: Navigating the Future of Computation, Challenges, and Technological Breakthroughs. Quantum Reports. 2024 Nov 16;6(4):627-63.

[237] Azhari R, Salsabila AN. Analyzing the Impact of Quantum Computing on Current Encryption Techniques. IAIC Transactions on Sustainable Digital Innovation (ITSDI). 2024 Feb 22;5(2):148-57.

[238] 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.

[239] Singh A, Dev K, Siljak H, Joshi HD, Magarini M. Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions. IEEE Communications Surveys & Tutorials. 2021 Sep 3;23(4):2218-47.

[240] Ashfaq S, Patil SA, Borde S, Chandre P, Shafi PM, Jadhav A. Zero Trust Security Paradigm: A Comprehensive Survey and Research Analysis. Journal of Electrical Systems. 2023 Jun 1;19(2).

[241] Ahuja B, Prabha C, Garg G. Emerging Technologies in E-Commerce Security. Strategic Innovations of AI and ML for E-Commerce Data Security. 2025:235-60.

[242] Arshad RU. The Evolution of E-Commerce: Emerging Trends and Consumer Behaviors in the Digital Marketplace. Research Corridor Journal of Engineering Science. 2024 Sep 23;1(2):166-81.

[243] Iwasokun GB, Omomule TG, Akinyede RO. Encryption and tokenization-based system for credit card information security. International Journal of Cyber Security and Digital Forensics. 2018 Sep 1;7(3):283-93.

[244] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[245] Lin H. Ethical and Scalable Automation: A Governance and Compliance Framework for Business Applications. arXiv preprint arXiv:2409.16872. 2024 Sep 25.

[246] Kommisetty PD, Abhireddy N. Cloud Migration Strategies: Ensuring Seamless Integration and Scalability in Dynamic Business Environments. International Journal of Engineering and Computer Science. 2024 Apr;13(04):26146-56.

[247] Achar S. Cloud computing security for multi-cloud service providers: Controls and techniques in our modern threat landscape. International Journal of Computer and Systems Engineering. 2022 Sep 13;16(9):379-84.

[248] Saha S, Mazumdar B. Towards Resolving Privacy and Security Issues in IoT-Based Cloud Computing Platforms for Smart City Applications. InIntegration of IoT with Cloud Computing for Smart Applications 2023 Jul 25 (pp. 53-80). Chapman and Hall/CRC.

[249] 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).

[250] Gupta U, Somani P, Behare N, Mahajan R, Singh M, Iyer CV. Revolutionizing Retail: IoT Applications for Enhanced Customer Experience. InInternet of Things Applications and Technology 2024 Sep 23 (pp. 60-80). Auerbach Publications.

[251] Tawalbeh LA, Muheidat F, Tawalbeh M, Quwaider M. IoT Privacy and security: Challenges and solutions. Applied Sciences. 2020 Jun 15;10(12):4102.

[252] Karale A. The challenges of IoT addressing security, ethics, privacy, and laws. Internet of Things. 2021 Sep 1; 15:100420.

[253] Abdul-Ghani HA, Konstantas D. A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective. Journal of Sensor and Actuator Networks. 2019 Apr 22;8(2):22.

[254] Ahmad AY, Verma N, Sarhan N, Awwad EM, Arora A, Nyangaresi VO. An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model. IEEE Access. 2024 Mar 18.

[255] Mizambekov C. The Ethical Implications of AI in E-commerce: Balancing Innovation and Responsibility. Emerging Science Research. 2024 Dec 20:14-24.

[256] Wei L, Xia Z. Big Data-Driven Personalization in E-Commerce: Algorithms, Privacy Concerns, and Consumer Behavior Implications. International Journal of Applied Machine Learning and Computational Intelligence. 2022 Apr 14;12(4).

[257] Staab R, Jovanović N, Balunović M, Vechev M. From principle to practice: Vertical data minimization for machine learning. In2024 IEEE Symposium on Security and Privacy (SP) 2024 May 19 (pp. 4733-4752). IEEE.

[258] Feretzakis G, Papaspyridis K, Gkoulalas-Divanis A, Verykios VS. Privacy-Preserving Techniques in Generative AI and Large Language Models: A Narrative Review. Information. 2024 Nov 4;15(11):697.

[259] Goyal HR, Vanitha A, Karthikeyan T, Adhikary P, Saranya R, Kumar SK. Enhancing Data Privacy in IoT Cloud Environments with Trust Management. In2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST) 2024 Apr 9 (pp. 143-148). IEEE.