Assignment 9

1. Investigate the regulatory landscape governing e-commerce security and data privacy, including GDPR, CCPA, and PCI DSS standards. Assess the impact of these regulations on e-commerce businesses and their compliance requirements. Develop a compliance framework and best practices for handling customer data, ensuring data privacy, obtaining consent, and maintaining transparency in data collection and processing practice

The rapid evolution of ecommerce has made privacy compliance a critical concern for many online businesses. With the increasing number of data breaches, consumer awareness, and fines for non-compliance, safeguarding customers' data and respecting their privacy has become a new standard.

According to Gartner, **75% of global consumers will have their personal data protected by privacy laws by the end of 2023**. This means a rise from 10% in 2020.

Understanding and meeting the legal obligations surrounding privacy in ecommerce is a necessity that allows you to grow and build trust among your clients.
In this **the most important laws and regulations concerning privacy compliance in ecommerce**. We will also show you the dos and don'ts of compliance and introduce you to privacy-driven analytics.

What is ecommerce compliance?

In simple terms, **ecommerce compliance means adhering to the rules governing ecommerce activities in the markets you sell in**. These include but are not limited to ecommerce regulations *per se*, data privacy regulations, online payment standards, accessibility norms, and the avoidance of dark patterns.

Investing in your ecommerce business' compliance is undoubtedly worth the sweat. A 2021 study by Cisco showed that 79% of consumers consider privacy compliance a buying factor

Ecommerce regulations

General Data Protection Regulation (GDPR)

Covered area: European Economic Area (EEA)

In May 2018, GDPR replaced the 1995 European Data Protection Directive (95/46EC). GDPR gives **individuals complete control over their personal data**. It also **strengthens and unifies rules governing data collection** from individuals within the European Union.

The regulation sets out **procedures for data handling, transparency, documentation, and user consent**, forcing organizations to keep records of and monitor all activities related to processing personal data.

The notion of personal data is comprehensive under GDPR. It refers to **any information that relates to a natural person and allows identifying them**. These stretch way further than a person's name, surname, and location – they also include online identifiers like IP addresses, cookies, as well as factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

Non-compliance exposes your business to **fines reaching up to 4% of your annual turnover**. In some cases, these can amount to millions of euros.

Steps to GDPR-compliant ecommerce:

1. **Map all types of personal data you collect** – including cookies and unique identifiers used in your data platforms, such as analytics, CRM, etc.

Limit your data collection to the minimum data necessary to fulfil a certain purpose.

CCPA & CPRA

Covered area: California, United States

The California Consumer Privacy Act (CCPA) is the original privacy act enforced in California that revolutionized the approach to data privacy in the US. This legislation was altered and expanded with the introduction of the California Privacy Rights Act (CPRA) which came into force on January 1, 2023

Your ecommerce business falls under CPRA regulations if:

- It has gross annual revenue greater than or equal to **$25 million.**
- It obtains information from **100,000 or more** California residents/households or devices annually.
- It generates at least **50%** of annual income from sharing or selling the information of California residents.

Furthermore, it also depends on the type of information that you process. If the data falls within the categories of personal information or sensitive personal information, as defined by the CPRA, you are bound by the law. To learn more about these types of data, consult the following chapters of our CCPA & CPRA article:

If your ecommerce business operates in California and meets the above criteria, you should take steps to comply with the CPRA.

Steps to CPRA-compliant ecommerce:

1. **Map your data and its sources.** This refers to every information about your customers gathered by marketing and sales tools.

2. **Ensure that the data is well-prepared** for your clients' access, deletion, and portability requests. If your marketing software vendor cannot fulfill these requirements, consider switching to a more privacy-oriented one.

3. **Check your third-party data sources.** If your company buys data, ensure it comes from legitimate, legal sources. Non-compliance may result in hefty fines.

4. **Create a process for handling customer requests.** Provide at least two methods for consumers to make their requests: a toll-free number and an online form.

5. **Provide a clear and understandable opt-out request form.** Place it on your homepage with the text *Do Not Sell or Share My Personal Information*.

6. **Give consumers the option to submit requests to:** delete their personal information, learn how it was collected, transfer it to another entity, and limit its use and disclosure.

7. **Update your privacy policy.** It should describe the rights of California residents. You can follow these guidelines on Making Your CCPA Privacy Policy Compliant with the CPRA.

   Watch out for updates to the law. Just like the CCPA, the CPRA may be updated after some time. There's already a bill proposal called the American Data Privacy and Protection Act (ADPPA)

The Digital Services Act

Covered area: EU

On December 15, 2020, the European Commission introduced the Digital Services Act (DSA) that entered into force on November 16, 2022. The act replaced and enhanced the e-Commerce Directive – a regulation that, back in 2000, set the foundational legal framework for online services in the EU.

The DSA aims to create a safer digital space that protects the users' rights. **It applies to all digital services that connect consumers to goods, services, or content**. This includes online marketplaces.

The DSA is meant to improve social media content moderation and protect users from illegal content, goods, and services. Thanks to the act, citizens will better control **how online platforms and big-tech companies use their data**.

It also gives the European Commission the right to demand **access to the algorithms of platforms** to ensure transparency in how they recommend content to their users. It obliges the platforms to **label all ads and inform users** about the entities promoting them.

Finally, the new regulations require platforms to provide a plain-language summary of their terms and conditions for easy understanding.

Steps to a DSA-compliant ecommerce:

1. Provide users with clear information on why they are recommended certain information.

2. Enable users to exercise **the right to opt out from recommendation systems based on profiling.**

3. Enable users to exercise **the right to complain to the platform, seek out-of-court settlements**, complain to their national authority in their language, or **seek compensation for breaches** of the rules.

4. Don’t display **advertisements based on sensitive user data** such as ethnic origin, political opinions, or sexual orientation.

5. Don’t use **profiling towards children** and display advertisements on that basis.

6. Don’t use the so-called ‘**dark patterns**‘in the interface of online platforms. This refers to design choices that manipulate users into decisions they don’t intend to make.

7. The EU states that the Digital Services Act will help small and medium-sized businesses and startups expand beyond their home market. This is because it reduces the costs of complying with 27 different laws across Europe.

   So far, the member states have regulated these services differently. This created barriers for smaller companies looking to expand and scale up across the EU and resulted in different levels of protection for Europeans.

ePrivacy Directive

Covered area: European Economic Area (EEA)

The ePrivacy Directive, also known as the "cookie law", was passed by the European Union in 2002 and amended in 2009. It governs **the use of cookies and the processing of personal data on websites**.

Since its enforcement, websites frequented by EU visitors **have to obtain explicit user consent before activating any cookies or trackers** that aren't strictly necessary for the core functioning of the website and services.

But there's more to that. Your website also has to:

- Ask for cookie consent **in a user-friendly way**.
- Inform the end-users about all cookies and trackers your website uses **in understandable, plain language**.
- Inform them about **the purposes of data processing** as well as **data storage, retention, and access**.
- Make the **withdrawal of cookie consent as easy as its submission**.

Because of the ePrivacy Directive, your website must present a cookie banner in the EU, giving European visitors more control over their personal data.

Despite being nicknamed the "cookie law", the ePrivacy Directive is not an actual law. It is a legislative act that sets out a goal all EU countries must achieve and implement locally. However, it's up to the EU countries how they accomplish these goals. Therefore, you should seek more guidance on the local implementation of the directive in the countries you run your business.

ePrivacy Regulation is a draft regulation proposed by the European Commission that **will replace the ePrivacy Directive** in the future. It will

update the current rules for using modern technology and adapt them to GDPR.

The new regulation will impose stricter rules for electronic communications and cover services such as Skype, WhatsApp and Facebook Messenger, Gmail, iMessage, or Viber. The goal is to prevent communication apps and internet services from intercepting, recording, or tapping into user messages.

Other key provisions of the proposed ePrivacy Regulation include:

- **The same level of protection** of electronic communication for all people and businesses and **a single set of rules for companies** across the EU
- **Protection of metadata** – the information that describes other pieces of data, such as author, date, location, etc. Metadata should be anonymized or deleted if visitors don't allow its use. The exception includes data necessary for billing.
- **Simpler rules for cookies.** Introducing user-friendly browser settings provides an easy way to accept or refuse tracking cookies and other identifiers. No consent is required for cookies that improve the internet experience, such as by saving shopping cart history or counting website visitors.
- **Protection against spam. The regulation will ban unsolicited electronic communications by email, SMS, and automated calling machines.**
- **More effective enforcement.** Like with GDPR, data protection authorities will be responsible for enforcing the new regulation rules.

The ePrivacy Regulation is still in the legislative process, and its effective date remains unknown. But one thing is for sure: **cookies and consent will stay**.

In November 2023, the European Data Protection Board (EDPB) formulated guidelines outlining the new technical scope of Art. 5 (3) of the ePrivacy Directive. According to this article, companies must obtain prior consent before storing or accessing information on a user's electronic device unless it is necessary to provide the requested service. So far, this principle has mainly applied to Internet cookies. **The recent guidelines significantly extend the list of technologies covered by Art. 5 (3) to include new tracking methods and technical operations.**

The EDPB focuses on five critical elements of the cookie rule and applies an extensive interpretation to all of them:

- **Information** includes both non-personal and personal data, regardless of how it is stored or by whom.
- **Terminal equipment** refers to equipment connected to the public telecommunications network, e.g., smartphones, laptops, connected cars, connected TVs, or smart glasses.
- **An electronic communications network** is any system that allows the transmission of electronic signals. The rule concerns public communication services provided over such networks. However, communication over a network available to a limited number of people (e.g., subscribers) is also considered public.
- **Access** – the EDPB has a very broad delimitation of access according to which an access exists if an entity actively takes steps to gain access to information stored on a terminal equipment.
- **Storage** applies to information of any type, in any quantity, and takes place over any time (even as short as storage in RAM or CPU cache).

PCI DSS (Payment Card Industry Data Security Standard):

PCI DSS is a set of security standards for businesses that handle payment card information. It applies to e-commerce businesses that accept credit or debit card payments.

The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the **security** of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. PCI DSS was designed to prevent cybersecurity breaches of sensitive data and reduce the risk of fraud for organizations that handle payment card information.

PCI DSS is not a law or legal regulatory requirement. However, it is often part of contractual obligations businesses that process and store credit, debit and other payment card transactions adhere to. Contractually obligated organizations must meet the requirements of PCI DSS to establish and maintain a secure environment for their clients.

PCI DSS was created in 2004 by five major credit card companies: Visa, MasterCard, Discover, JCB and American Express. The Payment Card Industry Security Standards Council (PCI SSC) developed the guidelines for PCI DSS.

Although not officially established until 2004, the history of PCI DSS' compliance framework began in the 1990s.

The purpose of PCI DSS

The primary goal of PCI DSS is to safeguard and optimize the security of sensitive cardholder data, such as credit card numbers, expiration dates and security codes. The standard's security controls help businesses minimize the risk of data breaches, fraud and identity theft.

Compliance with PCI DSS also ensures that businesses adhere to industry best practices when processing, storing and transmitting credit card data. In turn, PCI DSS compliance fosters trust among customers and stakeholders.

Six principles of PCI DSS

The PCI Security Standards Council (PCI SSC) has created six major goals for PCI DSS:

1. **Build and maintain a secure network and systems:** Credit card transactions must be conducted in a secure network. The security infrastructure should include **firewalls** that are strong and complex enough to be effective without causing inconvenience to cardholders or vendors. Specialized firewalls are available for wireless local area networks, which are highly vulnerable to eavesdropping and malicious attacks. Vendor-provided **authentication** data, such as personal identification numbers and passwords, should not be used on an ongoing basis.
2. **Protect cardholder data:** Organizations adhering to PCI DSS must protect cardholder information wherever it's stored. Repositories with vital data, such as birthdates, mothers' maiden names, Social Security numbers, phone numbers and mailing addresses, must be secure. The transmission of cardholder data through public networks must be **encrypted.**

3. **Maintain a vulnerability management program.** Card services organizations must institute risk assessment and vulnerability management programs that protect their systems from the activities of malicious hackers, such as spyware and malware. All applications should be free of bugs and vulnerabilities that might enable exploits in which cardholder data could be stolen or altered. Software and operating systems must be regularly updated and patched.
4. **Implement strong access control measures.** Access to system information and operations should be restricted and controlled. Every person who uses a computer in the system must be assigned a unique and confidential identification name or number. Cardholder data should be protected physically, as well as electronically. Physical protection can include the use of document shredders, limits on document duplication, locks on dumpsters and security measures at the point of sale.
5. **Regularly monitor and test networks.** Networks must be regularly monitored and tested to ensure security measures are in place, functioning properly and up to date. For example, antivirus and antispyware programs should be provided with the latest definitions and signatures. These programs frequently scan all exchanged data, applications and RAM and storage media.
6. **Maintain an information security policy.** A formal information security policy must be defined, maintained and followed by all participating entities. Enforcement measures, such as audits and penalties for noncompliance, might be necessary.

What are the 12 requirements of PCI DSS?

PCI SSC includes specific requirements in each of the six PCI DSS goals. Organizations that want to be PCI DSS-compliant must meet these 12 requirements:

1. Install and maintain a firewall to protect cardholder data environments.

2. Don't use vendor-supplied default passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt payment card data transmitted across open, public networks.
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data to employees with a business need because their jobs require access.
8. Assign a unique ID to each person with data or computer access.
9. Restrict who has physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain an **information security policy**.

PCI DSS compliance levels

PCI DSS compliance requirements are divided into four merchant levels, based on the annual volume of credit or debit card transactions processed by a business for both e-commerce and brick-and-mortar transactions. The following are the four validation levels:

1. **Level 1** includes organizations that handle more than 6 million card transactions a year. These businesses must pass a Qualified Security Assessor (QSA) assessment each year and have an Approved Scanning Vendor (ASV) do a quarterly network visibility scan.
2. **Level 2** includes organizations that handle from 1 million annual card transactions up to 6 million. They must complete an annual Self-Assessment Questionnaire (SAQ) and might be required to submit quarterly ASV network vulnerability scans.

3. **Level 3** includes organizations that handle more than 20,000 annual card transactions up to 1 million. Like level 2 businesses, level 3 businesses must complete an annual SAQ and might have to submit a quarterly network vulnerability scan.
4. **Level 4** includes organizations that handle fewer than 20,000 annual card transactions. Like levels 2 and 3, these businesses must complete an annual SAQ and might have to submit a quarterly network vulnerability scan.

Legal Requirements of E-commerce business in India

E-commerce broadly means a commercial activity conducted with the support of electronic devices. Under E-commerce, there are digital business transactions/trades which are wholly/partially performed by using the internet. As E-commerce has evolved and become more feasible and a safer way of shopping/trading, it is such an industry that requires a well-built regulatory framework in order to ensure accountability and consumer protection. The legal obligations to start an E-commerce business in India are as follows:

1. Company or LLP Registration

Every business is required to get registered with the Ministry of Corporate Affairs under the applicable laws. Such a business shall either be incorporated under the (Indian) Companies Act, 2013 or a foreign company or an office, branch or an agency outside India and necessarily be owned or controlled by an Indian resident.

While establishing an E-commerce business, it is suggested to have a company or LLP in place to relish the limited liability protection and at the same time, run a business with ease. Such registration ensures that the bank account is opened in the name of the company/ LLP which in return shall make the process of GST registration convenient and quicker.

As almost all marketplaces permit proprietorship and partnership firms to trade on their website, therefore, it is suggested to run the business through an LLP or a Company. In the event, where the promoters plan to establish an E-commerce website, as a Company it is the most suitable option as it is the only type of entity that have the access to angel funding or equity funding, which acts as a precondition to run a successful E-commerce business.

2. GST Registration

For a successful establishment of an E-commerce business, GST registration is mandatory. Every E-commerce business irrespective of its turnover is required to be compulsorily registered under the Central Goods & Service Tax (CGST) Act.

3. Bank Account

Opening a bank account in the name of the business is a convenient process. In case of a Proprietorship firm, the first step is to obtain a GST registration in the name of the business in order to open a bank account. An active bank account is the bare minimum requirement to be able to list a business on an E-commerce marketplace or to obtain a payment gateway for a proprietary E-commerce website.

4. Payment Gateway

A payment gateway is mandatory for a proprietary E-commerce website to process the payments. It allows the website to accept payments through credit card(s), debit card(s), net banking, internet banking from multiple banks. Therefore, one payment gateway is sufficient to accept various forms of online payments. Further, once the payment is received by the customer by the website, such payment is sent to that respective business's bank account through the payment gateway.

In the event, where the business runs through the online marketplaces, the marketplace would accept the payment through their payment gateway and directly credit such an amount to the bank account of the seller. Hence, a bank account shall be in place for smooth transactions.

5. Legal Documents

While selling on the internet, it is important to safeguard the business and the promoters by strict adherence to terms and conditions and the privacy policy of such businesses. In the case of a proprietary E-commerce website, the terms and conditions, disclaimer and privacy policy would have to be drafted as per the business, keeping in mind the nature of its activities and products they sell online.

If any business operates through online marketplaces, then the marketplace provides the seller with a legal document or sellers' agreement and the seller must abide by the sellers' agreement. It is important for any business to go through the sellers' agreement(s) in detail before the execution as it is the legal binding agreement between the seller and the marketplace.

Other requirements

There are a few additional requirements such as cyber law due diligence, compliance under the Competition Laws of India and the laws related to data protection and appointment of a Nodal Officer in case of an international E-commerce business setup in India which are important to always be complied with.

Compliances for E-commerce business in India

The trend of E-commerce has been rapidly increasing since the last decade. Many players with new business ideas have entered the market, be it Zomato/Swiggy delivering food from various restaurants or Flipkart/Amazon delivering products or Grofers delivering groceries.

The scenario is such that you name the service and there is an E-commerce platform for it available at the doorstep. The swift development of the E-commerce industry has called for the attention of the government towards forming regulations and policies with respect to the same. India has various laws that monitor E-commerce business in terms of data privacy, security of consumers, settlement transaction safety, quality of products etc.

1. Foreign Direct Investment

Foreign Direct Investment means the investment made by the foreign entities in the companies situated in India. The same can be done either by opening a subsidiary or associate in a foreign country, acquiring a controlling interest in an existing foreign company, or by means of a merger or joint venture with a foreign company. In India, the Ministry of Commerce and Industry, The Department of Industrial Policy and Promotion, Government of India form policy pronouncements on FDI. There are two ways to invest in India through FDI:

‘**Approval route**’ in which the prior permission of the central government is required before doing any foreign investment in India under a particular sector.

‘**Automated route**’ in which no prior permission is required and foreign entities can directly invest in Indian businesses under a particular sector.

The FDI policy allows Foreign Direct Investment to the extent of 100% in the marketplace model of E-commerce by the way of the Automatic Route. A single brand retail trading entity operating through brick-and-mortar stores is allowed to carry on retail trading through E-commerce. However, many E-commerce businesses have disguised their inventory-based model as a marketplace model through a complex structure.

2. Information Technologies Act, 2000

The E-commerce sellers conduct business in the same manner as the physical sellers with the only distinction of non-availability of the physical body in order to sell things. Through E-commerce, the vendors are required to generate bills, file returns, pay taxes, prepare ledgers and maintain records. They must perform all the same on the online platform.

The Information Technology Act, 2000 (IT Act) is the primary legislation that governs the use of the internet, cybercrime as well as the digital business in India. The IT Act governs online behaviour and related aspects of E-commerce and recognizes electronic contracts and digital signatures.

The Information Technology Act, 2000 is based on the Model Law of E-commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) and acts as a developing E-commerce enabling legislation in India. The Act targets regulating the use of the internet by punishing the person for publishing any obscene information or hacking or altering the data from devices of another person. The salient features of the Act are:

- E-contracts
- Transaction Security
- Digital signature

3. Payment and Settlements Systems Act, 2007

As per the Payment and Settlements Systems Act, the E-commerce business shall succeed as a payment system if it follows the Rules specified by RBI for online transactions and payments. Further, it is compulsory for an intermediary that is receiving payments through digital modes to have an active Nodal Account for settling the payments of the sellers on its E-commerce platform.

4. Consumer Protection Act, 2019

The E-commerce industry is also monitored by the Consumer Protection Act as it is working towards the interest of the consumers. In order to safeguard the consumers from unfair trade practices and further to address and solve their problems, the Ministry of Consumer Affairs, Food and Public Distribution on May 17, 2021, has notified the Consumer Protection (E-Commerce) Rules, 2021.

The rapid growth in the E-commerce industry is proof that E-commerce has become a vital and integral part of our lives. Long gone are the days where people used to hesitate from shopping online as they had doubts

about the quality, their money being stolen, non-delivery of the product. It is observed that today a huge part of the population trusts E-commerce websites for their day-to-day needs. Therefore, nowadays most of the purchases are prepaid compared to Cash on Delivery. This is a sign of the acceptance of E-commerce platforms by the general public especially during the COVID-19 pandemic, the usage of E-commerce has increased tremendously.

Our legal system is constantly introducing new rules and regulations to deal with this significant shift in the business model in order to safeguard the interest of the consumers. Therefore, a thorough understanding of the legal system and the possible problem(s) that an E-commerce business would face along with an effective risk management strategy is required for E-commerce businesses to thrive in this industry.

Best practices for handling customer data, ensuring data privacy, obtaining consent, and maintaining transparency in data collection

Most businesses hold personal information and conduct business on electronic devices. It's vital to the reputation and day-to-day running of your business that you keep the information safe and away from prying eyes. Don't be complacent – poor security can leave you and others vulnerable, and cyber-attacks affect businesses of all sizes.

Here are some practical steps you and your staff can take to improve your data security.

1. Back up your data

You **should** back up your data regularly. If you're using an external storage device, keep it somewhere other than your main workplace – encrypt it, and lock it away if possible. That way, if there's a break-in, fire or flood, you'll minimise the risk of losing all your data.

Check your back-up. You don't want to find out it's not worked when you need it most. Make sure your back-up isn't connected to your live data source, so that any malicious activity doesn't reach it.

2. Use strong passwords and multi-factor authentication

Make sure you use strong passwords on smartphones, laptops, tablets, email accounts and any other devices or accounts where personal information is stored. They **must** be difficult to guess. The National Cyber Security Centre (NCSC) recommends using three random words.

Where possible, you should consider using multi-factor authentication. Multi-factor authentication is a security measure to make sure the right person is accessing the data. It requires at least two separate forms of identification before access is granted. For example, you use a password and a one-time code which is sent by text message.

3. **Be aware of your surroundings**

   For example, if you're on a train or in a shared workspace, other people may be able to see your screen. A privacy screen might help you.

4. **Be wary of suspicious emails**

   You and your staff need to know how to spot suspicious emails. Look out for signs such as bad grammar, demands for you to act urgently and requests for payment. New technologies mean that email attacks are becoming more sophisticated. A phishing email could appear to come from a source you recognise. If you're not sure, speak to the sender. NCSC provide useful training materials to help you and your staff recognise suspicious emails.

5. **Install anti-virus and malware protection**

   And keep it up-to-date.

   You **must** make sure the devices you and your employees use at home, or when you're working away, are secure. Anti-virus software can help protect your device against malware sent through a phishing attack.

6. **Protect your device when it's unattended**

   Lock your screen when you're temporarily away from your desk to prevent someone else accessing your computer. If you do need to leave your device for longer, put it in a secure place, out of sight.

7. **Make sure your Wi-Fi connection is secure**

   Using public Wi-Fi, or an insecure connection, could put personal data at risk. You **should** make sure you always use a secure connection when connecting to the internet. If you're using a public network, consider using a secure Virtual Private Network (VPN).

8. **Limit access to those who need it**

Different workers may need to use different types of information. Put access controls in place to make sure people can only see the information they need. For example, payroll or HR may need to see workers' personal information, but your sales staff won't.

If someone leaves your company, or if they're absent for a long period of time, suspend their access to your systems.

9. Take care when sharing your screen

Sharing your screen in a virtual meeting may show your device to others exactly as you see it, including any open tabs or documents. Before sharing your screen, you **should** close anything you don't need and make sure your notifications and pop-up alerts are switched off.

10. Don't keep data for longer than you need it

Getting rid of data you no longer need will free up storage space. This also means you have less personal information at risk if you suffer a cyber-attack or personal data breach.

11. Dispose of old IT equipment and records securely

You **must** make sure no personal data is left on computers, laptops, smartphones or any other devices, before you dispose of them.
You **could** consider using deletion software, or hire a specialist to wipe the data.

Best practices for handling customer data, ensuring data privacy, obtaining consent, and maintaining transparency in data collection

1. Develop a written compliance framework that outlines data handling practices, privacy policies, and consent requirements specific to e-commerce.

2. Implement strong access controls and multi-factor authentication to ensure that only authorized individuals can access customer data.

3. Regularly review and update data handling and privacy policies to ensure compliance with e-commerce regulations and evolving customer expectations.

4. Obtain explicit consent from customers before collecting and processing their personal data, including through clear and prominent privacy policies and opt-in consent mechanisms.

5. Implement measures to protect customer data, such as encryption, secure storage, and regular backups, as well as protection against cyber threats and data breaches.

6. Provide transparency in data collection and processing practices, including informing customers about the types of data being collected, the purpose of data collection, and any third-party data sharing practices.

7. Establish incident response procedures to address any data breaches or unauthorized data access, including prompt notification to affected customers and regulatory authorities.

8. Regularly train employees on data privacy best practices and compliance requirements specific to e-commerce.

9. Conduct regular audits and assessments of data handling and privacy practices to ensure ongoing compliance and identify areas for improvement.

10. Consider appointing a data protection officer to oversee compliance with data privacy regulations and best practices specific to e-commerce.

11. Implement measures to ensure the security of payment information, such as using secure payment gateways and complying with Payment Card Industry Data Security Standard (PCI DSS).

12. Provide customers with clear and concise information about their data privacy rights and how to exercise them, such as through a clear and accessible privacy policy and opt-out mechanisms.

2. Explore the challenges and risks related to digital payment security, including unauthorized transactions, identity theft, and account takeovers. Evaluate current security measures such as encryption, tokenization, biometric authentication, and multi-factor authentication in mitigating fraud risks. a. Develop a comprehensive strategy to enhance digital payment security, including real-time transaction monitoring, fraud detection algorithms, customer education initiatives, and collaboration with financial institutions and cybersecurity experts

Digital payments have changed dramatically how the way money is handled, providing convenience and efficiency to all users around the world. As the usage of digital payment systems grows. There are significant security concerns. The purpose of this overview a full understanding of the existing landscape and suggest future research topics on security risks in digital payments. It accomplishes this by evaluating the body of knowledge and scholarly contributions made in this field. In order to understand security challenges, it is critical to examine the features and operation of digital payment systems.

Numerous studies have been conducted on various digital payment systems, such as mobile payments, internet banking, and crypto-currency exchanges. These studies highlight the procedures, protocols, and technologies employed in these systems, as well as any potential weaknesses that could be exploited by malicious actors.

A wide range of security concerns and attacks are revealed by the literature review to be directed at digital payment systems. The vulnerabilities present in the communication channels used for digital payments are a prominent field of research.

Studies indicates that we use encryption and authentication mechanism for unauthorised access or compromised system. Malwares most common threat are ransomware and banking Trojan, which can attack users on finance platform for their data.

Researchers have looked into the methods, capacities, and effects of various malware strains, providing insights into how they change over time and proposing mitigation tactics to combat them.

The study covers the topic of mobile payment systems and related security issues. It gives an overview of several mobile payment methods, including direct carrier billing, mobile payment platforms, independent mobile payment systems, mobile payment at the point of sale (POS), and mobile payment as the POS. The assessment underscores the usefulness and appeal of mobile payment systems but also draws attention to the security risks and difficulties they encounter. Additionally, the literature goes into great detail on the subject of fraud and identity theft in online transactions.

The invention of digital payments methods has resulted in various methods that manage financial transactions. The various technologies like from online shopping to mobile banking are the technologies providing speed simplicity, they allow customers to make payments anytime and anywhere. However, the people depend on digital platforms

The sensitive user data and financial information will be secured. We will explain about the complexities of digital payments security threats and vulnerabilities. It sparkles the light on the possible threats created by malware, particularly Trojan horses, which can penetrate user data and cause damage on digital platforms. It highlights some other security threats like DOS attacks, phishing, and malware that targets the user's personal information. Underlining the necessity for ongoing monitoring and proactive security measures and explore various authentication mechanisms in the digital payment system. It includes password authentication and two-factor authentication.

It talks about the significance of strong passwords, the danger of weak passwords and installation of additional verification processes to improve security. Moreover, it investigates the role of one-time password and biometric authentication such as facial recognition, fingerprint, in bolstering the security of digital payment transactions.

Encryption technique plays an important role in protecting the data during transactions. The paper looks into symmetric and asymmetric encryption algorithms, such as AES, 3DES, and RSA, stressing their relevance in preserving the security and integrity of sensitive information.

It also explores the hybrid encryption technique which combines both symmetric and asymmetric encryption to increase security measures. Furthermore, the paper addresses the significance of fraud detection and prevention in digital payments.

It helps to prevent fraud detection. It investigates the significance of secure transaction protocols such as tokenization in improving security and protecting sensitive data. Emerging technologies include block chain for secure transactions, artificial intelligence for fraud detection, and machine learning for pattern analysis.

Finally, this paper presents a detailed summary of digital payments security threats and vulnerabilities. Stakeholders can assure the confidentiality, integrity and authentication of transactions

By identifying the risks and implementing suitable security measures, eventually generating trust and confidence among users.

SECURITY THREATS AND SOLUTIONS

Security threats related to digital payment will evolve day by day. Some of common threats are Trojan. Trojan is malware where is acts as genuine software of the users but behaves the way it wants.

Trojan can reach users Personal computer (PC) or Phone through email along with PDF or downloadable links. It can track keystrokes, make system vulnerable to other attacks. It will change original data form, copy important information, update data if required, use system resources for its own task and hinder system performance. Comparing other viruses, Trojan don't have capability to duplicate itself.

Trojan can act in multiple ways, Backdoor Trojan where it will not attack your system instead will open doors for other attackers to manipulate your system, it achieves this by loading variety of malware to victim system which makes system vulnerable.

Rootkit will make sure that victim will not any malware on his/her system. Banking Trojans are those which captured screenshot during payment transaction with keystrokes capturing.

Remote access Trojan gives attacker a way to access victims system remotely, similar to banking Trojan even this can capture screenshot of transactions.

Trojan works in following,

- first it get downloaded to victim's system by escaping victim's awareness.

- Then Trojan gives remote working environment for attacker to deploy more malware to victim system.

- To this point victim system is under control of attacker.

- With respect to digital payment, attacker can target sensitive information like credit card details, transaction data, login and usage logs.

- They are good at hiding their presence on the victim system with the help rootkit type of virus.

  As mentioned earlier Trojan has capability to capture keystrokes which in turn leads to collect user credentials like username and password. In some cases it also captures screenshots, if you want context of screenshot with digital payment where attacker can take screenshot of transaction of victim.

Denial of service is the Cyber-attack where the third party tries to flood your system with hundreds of requests. This makes platform to break down and unable to provide service for users in turn recurring losses.

Worms are more dangerous because it does not need attacker intervention. It can act on its own, meaning it will duplicate itself and spreads across many devices.

One way it attacks is using Distributed denial of service (DDoS).In which it compromises as many as devices in the network and will flood the network as many request to bring the system eventually making financial loss to platform, service being unavailable to users.

In digital platform it can also take advantage of code not written properly, networks.

Phishing attacks comes Cyber threat where attackers act as trusted platform to communicate with unsuspecting user via mail, text or website. Attackers make sure he acts like trusted platform to get user credential or other sensitive information from the user.

Solution to prevent oneself from malware and attacks

Keep antivirus up to date.

Anti-virus companies' releases software updates regularly so with those software updates software can perform and detect new viruses in the market.

One more thing users can do is to use firewall which stands between device and foreign network ensuring logging of all activity. By enabling firewall will reduce the chances of system being compromised.

Users should be educated on where to download files; because Trojan are usually hidden in the PDF upon which downloading can transfer it system directly.

Make use of Encryption technique like SSL and TLS which encrypt connection between entities during transaction.

AUTHENTICATION MECHANISMS

In an era where digital payment systems are transforming our transaction methods, it is crucial to prioritize the implementation of strong security measures. This article explores the world of authentication mechanisms utilized in digital payment systems, providing insights into their importance and influence. By comprehending the advantages, drawbacks, and implementation factors associated with different authentication techniques, developers and users of payment systems can make well-informed choices to enhance security without compromising the convenience of seamless transactions.

Password-based:

Authentication is an important safety feature in digital payment systems, making password strength an important factor in making sure security in

general. This section addresses the importance of powerful passwords, the risks associated with weak ones, and ways for creating and managing strong passwords. In addition, it stresses the importance of password hashing n protecting user credentials, particularly in the event of data breaches.

Two-factor authentication, or 2FA for short, is an excellent way for improving security. Users must offer an additional form of verification in addition to their passwords in such a way. The paper examines several 2FA options, such as SMS codes, authentication apps, and bio-metrics, and assesses their usefulness in increasing security and limiting the risks of password leaks or theft.

To bolster security, incorporating two-factor authentication is highly recommended. This approach requires users to provide an additional form of verification beyond passwords. The article explores various 2FA methods, such as SMS codes, authentication apps, or bio-metrics, discussing their effectiveness in enhancing security and mitigating the risks of password breaches or theft.

One-time passwords offer an additional layer of security by generating unique codes for each transaction or login session. This section explains how OTP's work, their time-sensitive nature, and their resistance against replay attacks. It also explores the different methods of OTP generation, such as SMS, email, or dedicated mobile apps.

Bio-metric Identification:

Bio-metric authentication utilizes unique physical attributes, like fingerprints or facial features, to validate users' identities. The article discusses the advantages of bio-metrics, including their difficulty to replicate or forge. It highlights the integration of bio-metric authentication in mobile devices and payment apps, emphasizing the convenience and enhanced security it provides while minimizing the risk of credential theft.

ENCRYPTION TECHNIQUES

Encryption techniques play an important role in maintaining the security and privacy in digital payment systems. By applying many algorithms bland by doing so organizations can ensure the integrity, confidentiality, and authenticity of data during payment transactions. In this section, we will delve into the encryption techniques commonly utilized in digital

payment systems, highlighting their significance in bolstering security and privacy.

SYMMETRIC ENCRYPTION

Symmetric encryption stands as a foundational encryption technique widely embraced by digital payment systems. It operates by employing a single secret key for both encryption and decryption processes. This shared key between the sender and the recipient serves to establish secure communication channels and safeguard sensitive data. Notable symmetric encryption algorithms commonly employed in digital payment systems include:

AES (Advanced Encryption Standard): AES is widely called a symmetric block cipher due to its effective performance and strong security measures.

It supports key lengths of 128-bit, 192-bit, and 256- bit, providing a high level of encryption to ensure secure data transfer from one place to another.

3DES (Triple Data Encryption Standard):} On the other hand, 3DES uses the Data Encryption Standard (DES) algorithm by adding additional three consecutive encryption operations in a cascade. This approach enhances security by adding multiple layers of encryption to the data. While DES may be deemed relatively weak, the utilization of multiple encryption rounds within 3DES significantly bolsters security.

Symmetric encryption techniques enable the encryption of sensitive information, such as credit card details and transaction data, thereby guaranteeing its confidentiality and impeding unauthorized access.

ASYMMETRIC ENCRYPTION

Asymmetric encryption, also widely called public-key encryption, is an important technique used in digital payment systems. It operates using a pair of keys: a public key for encryption and a private key for decryption. While the public key can be freely shared, the private key is securely kept by the intended recipient. This approach ensures secure and unscathed communication between senders and receivers involved in digital transactions. The following benefits are provided by asymmetric encryption:

Secure Key Exchange: Asymmetric encryption helps in the secure exchange of keys between senders and receivers involved in a transaction. This ensures that session keys or symmetric encryption keys can be securely transmitted over any network, providing excellent protection against eavesdropping and unauthorized access.

Electronic Signatures: When ensuring the authenticity and integrity of digital price transactions, digital signatures are absolutely necessary. When a digital signature is created using the sender's private key, the recipient can use the corresponding public key to validate the signature.

Confidentiality: Confidentiality is another crucial feature provided by asymmetric encryption, which allows data to be encrypted using the sender's public key. Only the intended recipient, possessing the private key, can decrypt and gain access to the information, which significantly improves its confidentiality and privacy.

Prominent asymmetric encryption algorithms commonly utilized in digital payment systems include:

RSA (Rivest-Shamir-Adleman): RSA stands as a widely recognized encryption algorithm celebrated for its security and versatility in key exchange and digital signatures.

Elliptic Curve Cryptography (ECC): ECC offers robust security while employing shorter key lengths compared to traditional algorithms. This feature makes ECC particularly suitable for resource- constrained environments.

By implementing these encryption techniques, digital payment systems can fortify their security measures and safeguard sensitive data, ensuring a trustworthy and protected environment for payment transactions.

HYBRID ENCRYPTION

To harness the advantages of both symmetric and asymmetric encryption, hybrid encryption procedures are commonly utilized in digital payment systems. In this approach, symmetric encryption is used to encode the actual payment data, while asymmetric encryption is used to securely exchange and safeguard the symmetric encryption keys.

By combining these encryption techniques, digital payment systems can ensure secure and confidential transactions, safeguarding sensitive data from unauthorized access, alteration, and interception.

In conclusion, encryption techniques are vital components in addressing security and privacy concerns in digital payment systems. Symmetric encryption provides efficient and secure data transmission, while asymmetric encryption facilitates secure key exchange, digital signatures, and confidentiality. By employing hybrid encryption approaches, organizations can leverage the strengths of both techniques to enhance the security and privacy of digital payment transactions, thereby building trust and safeguarding sensitive information.

FRAUD DETECTION AND PREVENTION

Fraud detection is to take care of transaction occurring through internet. There are security concerns like unauthorized access is where person who does have any rights on platform access the platform like hackers and cyber criminals employ techniques like phishing and denial of service. Data breaches can happen when system is under control of attacker/ compromised, which attackers can get access to personal information like credentials.

Malware/ransomware will also cause a threat which can take control of victim's system.

Privacy concerns like data collection from user ensures that user on platform are legitimate. This can be ensured by collecting necessary details like transnational details, device information which are necessary for prevention and detection of frauds.

Data security should be implemented so user's data is intact so attacks on data is detected. Secure storage devices, encryption can help data security.

User should be consented for which data is collected from them so they understand why those data are collected. Data retention policies should be known to user and it is ethical role of data collectors to dispose data. User should have right to see, access, and update data collected by them to the platform.

Few measure are taken to prevent are Multi factor authentication and real time monitoring.

Two factor authentication adds one more step on entering password which user know and user were asked to link something like email or phone number which are belonging of user, where it significantly reduces the unauthorized user into someone else account. conventional method like entering password is vulnerable to phishing, brute force attack or social engineering.

In Two factor authentication,

first part is user password or user pin that user knows and want to keep it secret but the problem password faces is that is can be easily compromised using phishing or key logging. It can be easily figured out by cybercriminal.

Second part of Two factor authentication is thing which user owns and can be used to get entry to the platform. Commonly used factors are OPT, Notification sent to user phone. OTP (one time password) is sent to user's phone app, text or email which user can enter after entering password which send the second factor to you.

Real time monitoring tracks transaction currently happening over network or continuous monitoring of transaction either by collecting location, amount, user behaviour.

Key components of real time monitoring is transaction monitoring which use machine learning algorithm to analyse transaction. It includes velocity checks, outlier identification which helps to understand any behavior which is abnormal. Collects data from multiple sources where it includes data lie customer information, organization information which helps in fraud detection.

Behaviour analysis tries to read the history of user's transaction to verify their previous behaviour and current behaviour to identify any potential fraud and makes it easy to prevent it. Network monitoring is key component of real time monitoring where not only user's profile is monitored to prevent fraud but entire network is monitored to identify any distributed denial service of attack or any system breaches. But one more thing to remember is apart from the above key components constant improvement to identify new malware, new machine learning algorithms to analyses network or user profile should be discovered to mitigate new fraud and prevent it from occurring.

SECURE TRANSACTION PROTOCOLS

Encryption plays a crucial role in different applications, http is an extension it will add encryption for authentication laters. It will creates secure communication between client and server, it allows platforms exchange all the data during transactions through the network.

Encryption is a fundamental concept in modern cryptography. It will converts the data into unreadable form called cipher text. Symmetric key encryption is also called as secret key encryption.

The employs shared a single key for the both encryption and decryption process. It will encrypts the large amount of data. Asymmetric key is also known as public key encryption, the public key is freely distributed and used for encryption. Private Key is use for decryption, a sender can send a message using their private key, it is an authentication protocol developed by major payment card networks. It provides an extra layer of security for online card transactions. It allows the card holder's identity to be verified by providing an additional authentication step during the payment process.

This protocol may use of combination of cryptography techniques and dynamic data exchange between the card holders. It helps to make the secure transactions. It reduces the danger card fraud attacks and improves the security of digital payments.

It will add extra authentication to the payment process often mentioned as 3d secure authentication. it involves the three steps they are the issuer domain, the acquirer domain, the interoperability domain. When a card holder begins an online payment transactions, the merchant's website initiates the 3Ds process.

Tokenization is a technique during digital transactions it will substitute the sensitive card payment with unique tokens, it is a highly effective technique, and it offers a powerful solution by replacing sensitive data with unique tokens.

Tokenization offers various advantages for digital payments. it significantly reduces the risk and unauthorized access to sensitive payment card information, it enhances the security of data transmission during digital payment transactions.

Tokens are used as actual payment card data, the risk of compromising the data during transmission is greatly mitigated. Tokenization has become an accepted and widely adopted security measure in digital

payment systems it includes mobile payments, E-commerce, and recurring billing. By protecting critical payment card data and minimizing the possible effects of data breaches, it improves the overall security posture.

It is an advanced security measure, Bio-metric authentication utilizes special physiological such as face recognition, fingerprints. It is used to verify the identity during digital payment transaction. It will provide high level security of data.

When bio metric authentication is used during the payment process, unauthorized access risk can be minimized. It will protect the sensitive information. The user's payment account is connected to their bio metric data through bio-metric authentication.

When starting a transaction the user is to provide their bio-metric sample. such as putting their finger on a fingerprint. It will offers several advantages for digital payments Users are no longer required to type or remember complicated PIN's or passwords.

Instead, users may easily and rapidly authenticate themselves using their bio-metric traits, which are essentially individual to them. Replication of bio-metric authentication is challenging.

Bio-metric traits are intrinsically linked to the individual and are therefore impossible to copy or transmit, in contrast to passwords that can be lost, stolen, or exchanged and if offers a highly secure and convenient method for verifying the identity of users in electronic payment exchanges.

It improves security, lowers the possibility of unwanted access, and offers a user-friendly experience by utilizing special bio-metric traits. Bio-metric authentication is anticipated to play a bigger part in the future of secure digital payments as technology develops and bio- metric systems continue to advance.

It is critical to address the security threats posed by these platforms given the growing use of mobile devices for digital payments. The secure storing of payment credentials, data encryption during transmission, and defense against malware and illegal access are the main concerns of secure transaction protocols for mobile devices.

Some of the approaches used to strengthen the security of digital payments on mobile devices include mobile-based authentication apps,

secure components, and device fingerprinting. It is concerned with safeguarding the data saved on the device. It helps to secure data by transforming it into an unreadable format that can only be viewed with a decryption key. It encodes the sensitive payment data store on the device. The information is still shielded from unwanted access.

Application developer's overview the secure app development standards are essential for keeping mobile devices secure coding practices, conduct testing and include strong security measures into their applications.

The apps should utilize encryption Implement safe authentication procedures for data transmission, and overview to industry security requirements. It includes secure network connections when connecting public networks like Wi-Fi, the user must be aware this network Eavesdropping and man-in-the-middle attacks are possible. Use VPN network, it will establish secure and encrypted networks. It will protects the confidential data transmitted over the public network. It includes secure network connections when connecting public networks like Wi-Fi, the user must be aware this network Eavesdropping and man-in-the-middle attacks are possible.

Use VPN network, it will establish secure and encrypted networks. It will protects the confidential data transmitted over the public network. Device authentication and user awareness are all examples of mobile device Mobile devices may be trusted platforms for completing secure digital payment transactions while protecting sensitive payment information and user privacy by applying strong security measures.

EMERGING TECHNOLOGIES

Digital payment systems continue to develop new technologies are being created to improve user ease, experience, and efficiency however . It will explore some emerging technologies like that aims to address the concerns and it will improve the security and privacy in digital payment systems.

Tokenization is a technology, it replaces the sensitive data such as Credit card numbers, for example, can be replaced with unique tokens. Tokens are generated random there is no relationship between the original data, If an unauthorized entity intercepts the message.

Tokenization can help digital payment systems limit the danger of disclosing sensitive information during transactions it enhance the security and privacy.

Using the bio-metric authentication technology such as facial recognize and fingerprint, it will add an extra layer of security for digital payment system.

By utilizing distinct biological traits, these technology can verify the user identity with high level precision. Block chain is technology, this technology is originally developed for crypto-currency like **bitcoin** has gotten a lot of attention because of its potential to change digital payment methods.

It decentralize the nature enhances security and privacy. Block chain transactions are verified and it cannot be altered, by providing the robust frame for secure and digital payments.

Artificial intelligence is a technology, AI is used for fraud detection system with the help of machine learning algorithms, it is used to analyse huge amount of transaction data and used to identify the fraud relevant activities. These algorithms may learn and adapt to new fraud patterns in real time, increasing their accuracy over time.

Digital payment system in AI can detect proactively and prevent fraud transactions, ensuring the security and privacy of users' financial information.

Machine learning algorithms can continuously analyse and process the data. They are improving their comprehension of normal and deviant transaction behaviour. It enables AI systems to keep up with emerging fraud tactics. Increasing their effectiveness in detecting and preventing fraudulent transactions.

Finally the security and privacy problems in digital payments are substantial and must be addressed because security threats such as Trojans and phishing attacks are becoming more sophisticated, continues prevention measures and required user knowledge. It includes mechanisms like authentication, passwords-based and bio-metric methods plays an important role to verify the user identity and reduced unauthorized access.

Some of encryption techniques like symmetric and asymmetric encryption During transactions, maintain the confidentiality and integrity of sensitive data. Tokenization protects card information effectively while developing emerging technologies like block chain and Artificial intelligence contribute to improving the security and privacy of digital payment systems. Continuous research and development in these areas is critical for staying ahead of developing security risks and assuring the reliability and security of digital transactions.