



**RV College of
Engineering®**

Go, change the world

22EM106-Introduction to Cyber Security

UNIT- IV

E - Commerce and Digital Payments

Course Incharge: Dr.Mohana

Department of Computer Science & Engineering (Cyber Security)

RV College of Engineering, Bangalore-560059

Unit -IV**8 Hrs****E - Commerce and Digital Payments**

Definition of E- Commerce, Main components of E-Commerce, Elements of E-Commerce security, E-Commerce threats, E-Commerce security best practices, Introduction to digital payments, Components of digital payment and stake holders, Modes of digital payments- Banking

Cards, Unified Payment Interface (UPI), e-Wallets, Unstructured Supplementary Service Data (USSD), Aadhar enabled payments, Digital payments related common frauds and preventive measures. RBI guidelines on digital payments and customer protection in unauthorised banking transactions. Relevant provisions of Payment Settlement Act, 2007

- Ecommerce security refers to **the measures taken to protect your business and your customers against cyber threats.**
- E-Commerce or Electronic Commerce means **buying and selling of goods**, products or services over the internet.
- **electronic commerce or internet commerce.**
- These services provided online over the internet network.
- Transaction of money, funds, and data are also considered as E-commerce.
- Business to Business (B2B), Business to Customer (B2C), Customer to Customer (C2C), Customer to Business (C2B). The standard definition of E-commerce is a **commercial transaction which is happened over the internet.**

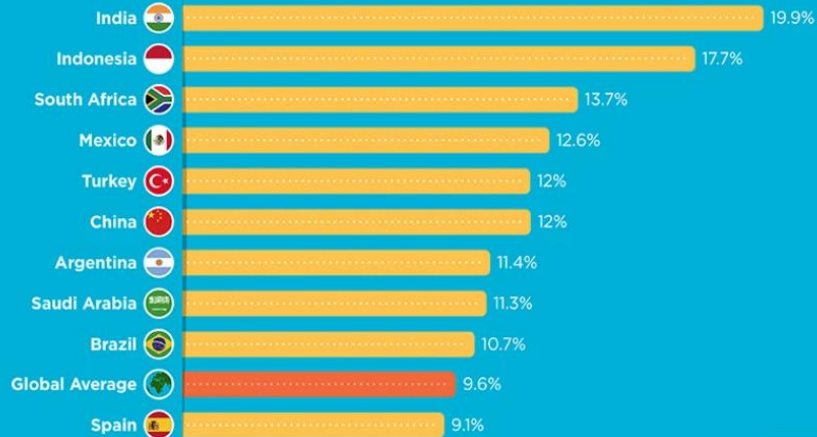
Examples of E-Commerce:

- Amazon
- Flipkart
- eBay
- Fiverr
- Upwork
- Olx
- Quikr

e-commerce is one of the fastest growing industries in the global economy



Ecommerce annual growth forecast



Top 10 Most Demanded & Hot Selling Products

In India Online 2021



Clothing



Cell Phones



Stationery & Books



Toys & Games



Footwear



Jewellery



Beauty & personal care



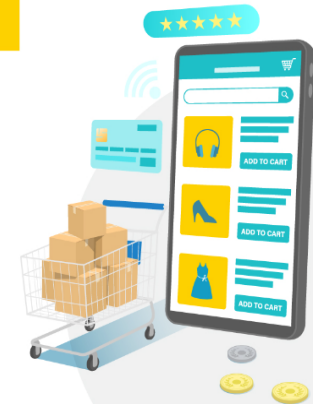
Electronics



Baby care products



Home Decor



1. Business to Business

Ex. online transactions only involve the manufacturers, wholesalers, retailers etc

2. Business to Consumer

Ex. Amazon, Flipkart, Jabong etc

3. Consumer to Consumer

Ex. OLX, Quikr

4. Consumer to Business

Ex. IT freelancer who demos and sells his software to a company.

- E-commerce provides the sellers with a global reach. They **remove the barrier of place** (geography) Now sellers and buyers **can meet in the virtual world**, without the hindrance of location.
- Electronic commerce will substantially **lower the transaction cost**. It eliminates many fixed costs of maintaining brick and mortar shops. This allows the companies to enjoy a much higher margin of profit.
- It provides quick delivery of goods with very little effort on part of the customer. complaints are also addressed quickly. It also **saves time, energy and effort** for both the consumers and the company.
- A customer **can shop 24×7**. The website is functional at all times, it **does not have working hours like a shop**.
- **without any intermediaries.**

- The **start-up costs** of the e-commerce portal are **very high**.
- Although it may seem like a sure thing, the **e-commerce industry has a high risk of failure**.
- At times, e-commerce can feel impersonal. lack of a personal touch can be a disadvantage for many types of **services and products like interior designing** or the jewelry business.
- Security is another area of concern. Only recently, we have witnessed many security breaches where the information of the customers was stolen. **Credit card theft, identity theft etc. remain big concerns with the customers.**
- Then there are also **fulfilment problems**. Even after the order is placed there can be problems with shipping, delivery, mix-ups etc. This **leaves the customers unhappy and dissatisfied**.

- It allows to **protect company and customers** from cybercriminals.
- cybersecurity is a concept that encompasses a **set of strategies, tactics and technologies that aim to defend systems**, digital services and online electronic data belonging to consumers, institutions and companies against theft, manipulation, blocking, disorientation and other damage caused by cybercriminals.
- primarily aimed at **protecting consumer data**.
- **Prevent data** such as **address, telephone, CPF, credit card numbers and navigation data**.
- cybersecurity must be dedicated to **protecting servers, databases, networks and endpoints**.
- It must **find vulnerabilities and fix them before cybercriminals do**.

cybersecurity is premised on ensuring:

- **Reliability:** only **authorized persons** can have access to systems and data;
- **Integrity:** data **cannot be altered or deleted** without authorization;
- **Authenticity:** The **identity of the people** who send data to your company must be preserved.

- Protect **company and customers** from cybercriminals.
- In order for people to be able to shop at your online store, they need to **feel secure enough to enter personal details and payment details.**
- customers' **data and customer's information** need to be careful.
- Have a cyber security **policy** in place
- Create **strong passphrases**
- Use a **secure e-commerce platform**
- Don't **fall for phishing scams**

<http://www.cert-in.org.in/>

https://cert-in.org.in/s2cMainServlet?pageid=Pre_Sec_Tips1

<https://cert-in.org.in/>



The screenshot shows the official website of the Indian Computer Emergency Response Team (CERT-In). The header includes the organization's name, logo, and navigation links. The main content area features a welcome message, a list of functions, and a section for the latest security alerts. The left sidebar contains various logos and partner information.

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

certin
Enhancing Cyber Security in India

HOME ABOUT CERT-In KNOWLEDGEBASE TRAINING ADVISORIES VULNERABILITY NOTES CYBER SECURITY ASSURANCE

Welcome to CERT-In

CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

In the Information Technology Amendment Act 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed

Latest Security Alert

- CERT-In Vulnerability Note CIVN-2023-0061** (February 24, 2023)
Weak Key Protection Vulnerability in Siemens SINUMERIK ONE and SINUMERIK MC
- CERT-In Vulnerability Note CIVN-2023-0060** (February 24, 2023)
Multiple vulnerabilities in VMware products
- CERT-In Vulnerability Note CIVN-2023-0059** (February 23, 2023)

Current Activities

- Exchange server 2013 End of Support** (February 22, 2023)
Microsoft Exchange Server 2013 will enter its End of Life on Tuesday, April 11, 2023 which means that Microsoft will no longer be offering technical support and updates of security [More >>]
- Threat actors exploiting authentication bypass vulnerability in Fortinet Products** (December 05, 2022)
It is reported that threat actors are actively exploiting an

Left Sidebar:

- G20 India 2023
- संयुक्त सुरक्षा केंद्र
- Digital India
- साइबर स्वच्छता केन्द्र
- CYBER SWACHHTA KENDRA
- Botnet Cleaning and Malware Analysis Centre
- Full Member: FIRST
- Operational Member: APCERT
- Accredited Member: TF-CSIRT
- Global Research Partner: IAPWG
- Directions by CERT-In under Section 70B, Information Technology Act 2008



TYPE Conceptual Analysis
PUBLISHED 19 October 2022
DOI 10.3389/fpsyg.2022.927398



OPEN ACCESS

EDITED BY
Umair Akram,
RMIT University, Vietnam

Cyber security threats: A never-ending challenge for e-commerce

- -commerce workflow
- Identify the various cybersecurity threats in e-commerce
- How cybersecurity threats can be addressed and minimized?



- Most industries have **deployed internet technologies** as an **essential part of their business operations**.
- online banking customers the facilities to access and manage their bank accounts easily and globally.
- Deployed more **frequently over the past few decades to support and improve the operational and managerial performance**
- internet banking, e-banking or virtual banking

- Confidentiality, privacy and security of internet banking transactions and personal information are the major concerns.
- steal login data.
- Phishing, pharming, Cross-site scripting, adware, key loggers, malware, spyware, Trojans and viruses.

- Protect your PC.
- Protect your personal information
- Use the Internet cautiously
- Stay alert
- Prompt reporting of suspicious activity

Protect your PC:

- Anti-virus software, anti-spyware security software, **firewalls, operating system and internet browser up to date**

Protect your personal information:

- hard-to-guess security access codes
- Change your security access codes **periodically**
- Memorize your security access codes, **avoid writing** them down
- Do not disclose to ANYONE your security access codes
- Never leave your PC unattended when logged into Online Banking
- "Log-off" button when finished using the e-banking services

Use the Internet cautiously:

- Always access Online Banking internet **only by typing the URL** in the address bar of your browser.
- Never attempt to access Online Banking internet through an **external link of unknown or suspicious origin appearing on other websites**, search engines or e-mails.
- check for the Bank's Security Certificate details and the various signs (e.g., green address line and Lock, HTTPs)
- Ignore and delete immediately **suspicious fraudulent e-mails**
- Never click on a **link contained in suspicious e-mails**
- Avoid using Online Banking from **public shared PCs**

Stay alert:

- Sign-on to Online Banking **regularly and review your account transactions**, checking for any fraudulent activity on your account (e.g. transactions you do not recognize)
- Keep track of your **last log-on date and time**, displayed at the top left side of the Online Banking Home page
- Once logged into Online Banking, you can also **monitor the actions performed online**

Prompt reporting of suspicious activity:

- Contact your bank immediately, if you think **someone knows your security access code** or in case of **theft of your code/ money** or in case you have forgotten your credentials.
- Forward any suspicious e-mails to the bank on their **phishing reporting** email as well as on CERT-In email **incident@cert-in.org.in**
- Your prompt action is crucial to prevent any (further) damage

- usage of Smartphones
- use of a Smartphone or other cellular device to perform online banking tasks

Mobile Banking Malwares

prevention against Malware attacks:

- Download and use anti-malware protection for the mobile phone or tablet device.
- Keep the Banking App software up to date
- Use security software.
- Reputed applications should only be download onto the smart phone

An attacker attempts phishing on to a mobile phone **through SMS** (Short Message Service), text message, telephone call, fax, voicemail etc. with a purpose to **convince the recipients to share their sensitive or personal** information.

- Emails or text messages asking the **user to confirm or provide personal information** (Debit/Credit/ATM pin, CVV, expiry date, passwords, etc.) should be ignored.
- SSL (Secure Sockets Layer) and TLS (Transport Layer Security) should be **adequately implemented in mobile banking apps thus** helping to prevent phishing and man-in-the-middle attacks.

- Enable Passwords On Devices
- IPIN should **not be stored** on the user's mobile phone.
- report the **loss of mobile phone** to the bank for them to disable the user's IPIN and his access to the bank's account through Mobile Banking app.
- When downloading the Bank's Mobile app in the mobile device, the user **should go to a trusted source** such as the App Store on the iPhone® and iPod touch® or Android Market.

Security Threats

- Identity theft
- The fraudulent acquisition and use of **person's private identifying information, usually for financial gain.**
- It can be divided into two broad categories: Application fraud and Account takeover

Application fraud:

- criminal uses stolen or fake documents to open an account in someone else's name.
- Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information.

Account takeover:

- criminal tries to take over another person's account, first by gathering information about the intended victim, and then contacting their card issuer while impersonating the genuine cardholder, and asking for the mail to be redirected to a new address.
- The criminal then reports the card loss and asks for a replacement to be sent.



- electronic payment
- phone, POS (Point of Sales) or computer, a digital channel communications
- funds are transferred **much faster** relative to traditional payment methods like checks.
- ePayments allow users to make payments **online at any time, from anywhere in the world**, and also remove the need to go to banks.
- As part of the '**Digital India**' campaign, the government has an aim to create a 'digitally empowered' economy that is '**Faceless, Paperless, Cashless**'.

- Banking Cards
- Unstructured Supplementary Service Data(USSD)
- Aadhaar Enabled Payment System (AEPS)
- Unified Payments Interface (UPI)
- Mobile Wallets
- Bank Prepaid Cards
- PoS Terminals
- Internet Banking
- Mobile Banking
- Micro ATMs

- **Ease and convenience**
- **Economic progress**
- **Safety and efficient tracking**
- Online retail provides an additional sales channel.
- Improved cash flow.
- Security at the forefront.
- Improved payment options for your customers.
- **Multiple payment options:** Several types of payment modes including credit cards, debit cards, net banking, EMIs, and UPI, along with Paytm Wallet and Paytm Postpaid.
-

- Debit/credit cards, or prepaid cards.
- [Andhra Bank](#) launched the first credit card in India in [1981](#).
- Cards are preferred because of multiple reasons

- USSD was launched for those sections of India's population which **don't have access to proper banking and internet facilities.**
- Under USSD, mobile banking transactions are possible without an internet connection by simply **dialing *99# on any essential feature phone.**
- allows customers to **avail of services including interbank account** to account fund transfer, balance inquiry, and availing mini statements.
- Around 51 leading banks offer USSD service in **12 different languages**, including Hindi & English.

- Under this system, customers can use their **Aadhaar-linked accounts to transfer money** between two Aadhaar linked Bank Accounts.
- As of February 2020, AEPS had crossed more than **205 million** as per NPCI data.
- AEPS **doesn't require any physical activity** like visiting a branch, using debit or credit cards or making a signature on a document.
- This bank-led model allows digital payments at PoS (Point of Sale / Micro ATM) via a Business Correspondent(also known as Bank Mitra) using Aadhaar authentication.

- UPI is a payment system that culminates numerous bank accounts into a single application, allowing the transfer of money easily between any two parties.
- As compared to NEFT, RTGS, and IMPS, UPI is far more well-defined and standardized across banks.
- You can use UPI to initiate a bank transfer from anywhere in just a few clicks.
- The benefit of using UPI is that it allows you to pay directly from your bank account, without the need to type in the card or bank details.
- This method has become one of the most popular digital payment modes in 2020, with October witnessing over 2 billion transactions.

- type of wallet in which you can carry cash but in a digital format.
- Often customers **link their bank accounts or banking cards** to the wallet to facilitate secure digital transactions.
- Another way to use wallets is to **add money to the Mobile Wallet** and use the said balance to transfer money.
- Some popularly used ones **include Paytm, Freecharge, Mobikwik, mRupee, Vodafone M-Pesa, Airtel Money, Jio Money, SBI Buddy, Vodafone M-Pesa, Axis Bank Lime, ICICI Pockets, etc.**

- A bank prepaid card is a pre-loaded debit card issued by a bank, usually **single-use or reloadable for multiple uses**.
- It is different from a standard debit card because the **latter is always linked with your bank account and can be used numerous times**. This may or may not apply to a prepaid bank card.
- A prepaid card can be created by any customer who has a KYC-complied account by merely visiting the bank's website.
- **Corporate gifts, reward cards, or single-use cards for gifting purposes** are the most common uses of these cards.

- PoS(Point of Sale) is known as the location or segment where a sale happens.
- The most common type of PoS **machine is for Debit and Credit cards**, where customers can **make payment by simply swiping the card and entering the PIN**.
- With digitization and the increasing popularity of other online payment methods, new PoS methods have come into the picture. First is the **contactless reader of a PoS machine, which can debit any amount up to Rs. 2000** by auto-authenticating it, without the need of a Card PIN.

- Internet Banking, also known as e-banking or online banking, allows the customers of a particular bank to make transactions and conduct other financial activities via the bank's website.
- E-banking requires a steady internet connection to make or receive payments and access a bank's website, which is called Internet Banking.
- Today, most Indian banks have launched their internet banking services. It has become one of the most popular means of online transactions.
- Every payment gateway in India has a virtual banking option available. NEFT, RTGS, or IMPS are some of the top ways to make transactions via internet banking.

- Digital payment methods, such as IMPS, NEFT, [RTGS](#), IMPS, investments, bank statements, bill payments, etc., are available on a single platform in mobile banking apps.
- Banks themselves encourage customers to go digital as it makes processes easier for them too.

Modes of digital payments- Banking

<https://www.meity.gov.in/modes-digital-payment>

<https://www.meity.gov.in/cyber-security-division>

- Modes of Digital Payments.
- Unified Payments Interface (UPI):
- Bharat Interface for Money (BHIM):
- UPI 123PAY:
- UPI Lite:
- Cards (including RuPay Debit Cards)
- Immediate Payment Services (IMPS):
- Aadhaar Enabled Payment System (AePS):



Thank you