E-Commerce in Past, Present and Future

BY

SHAIK KHAJA MOHIDDDIN,
RESEARCH SCHOLAR IN ANU,
ASSO.PROF. AT VVIT, NAMBUR, GUNTUR.

Mail id: mail2mohiddin@gmail.com
E-COMMERCE

• PAST

• PRESENT

• FUTURE
History of E-Commerce

• The rise of internet companies in India started in the mid-1990s.
• The first Indian internet companies mainly featured online classifieds, matrimonial and job portals.
• The low penetration of internet, lack of awareness and lack of development and confidence in online payment systems were reasons for Indian internet companies not actively engaging in e-commerce.
• It was only in the mid-2000s, after the dot com bubble burst that e-commerce industry in India started to take off.
• The first e-commerce services available were mainly offered in the travel industry. With the proliferation of low cost carrier airlines, ticket offering started to be made online.
• Even today travel booking websites hold a majority share of the Indian e-commerce space
E-commerce space relating to the deals and discounts websites started becoming popular towards 2009 and onwards while the concept of social media for e-commerce is still trying to make a foothold in the markets despite having one of the largest populations using Facebook.
Between 2000 and 2005: The first wave of E-Commerce in India was characterized by a small online shopping user base, low internet penetration, slow internet speed, low consumer acceptance of online shopping and inadequate logistics infrastructure.
Between 2005 and 2010: There were basically two major transitions that took place that aided in the build of E-Commerce story in India.

**Online Travel**: The entry of Low Cost Carriers (LCCs) in the Indian aviation sector in 2005 marked the beginning of the second wave of e-Commerce in India.

**Online Retail**: The growth of online retail was partly driven by changing urban consumer lifestyle and the need for convenience of shopping at home.
2010 onwards:

- **Group buying**: Starting in 2010, the group buying and daily deals models became a sought after space for entrepreneurs in India, emulating the global trend.
- **Social Commerce**: It is a key avenue for E-Commerce players to reach out to target customers.
- **Present Scenario**: India’s E-Commerce market grew at a staggering 88% in 2013 to $16 billion, riding on booming online retail trends.
1st wave (1996-2000)

- Launch of internet in India via dialup in 6 cities
- Launch of online job portals
- Muted activity in the industry due to the dotcom bubble in 2000

2nd wave (2006-present)

- Entry of a number of players in e-tailing segment
- Launch of online B2B portals
- Launch of online matrimonial portals
- Launch of online travel agents (OTAs)
- Launch of first group buying website in India
- New trend of use of social networking sites (SNS) as a marketing tool begins or the advent of social commerce
Can anybody tell me the earliest example of e-business or e-commerce?
SITA
SWIFT
SITA-Society Internationale de Télécommunications Aéronautiques, was founded in February 1949 by 11 airlines
SWIFT – Society for Worldwide Interbank Financial Telecommunication was founded in 1973. Today it is linked to more than 50000 financial institutions in more than 400 countries, & carries 15 million messages per day.
e-Commerce history

• Mid-1990s to 2000: rapid growth
“Dot-com boom” followed by “dot-com bust”
• 2000 to 2003: overly gloomy news reports
• 2003: signs of new life
  Sales and profit growth return
e-Commerce growing at a rapid pace
e-Commerce becomes part of general economy
• 2008 – 2009 general recession
  Electronic commerce hurt less than most of economy
• Post 2009 – 2nd Wave / E-Commerce 2.0 underway
<table>
<thead>
<tr>
<th>Electronic Commerce Characteristic</th>
<th>First Wave</th>
<th>Second Wave</th>
</tr>
</thead>
<tbody>
<tr>
<td>International character of electronic commerce</td>
<td>Dominated by U.S. companies</td>
<td>Global enterprises in many countries participating in electronic commerce</td>
</tr>
<tr>
<td>Languages</td>
<td>Most electronic commerce Web sites in English</td>
<td>Many electronic commerce Web sites available in multiple languages</td>
</tr>
<tr>
<td>Funding</td>
<td>Many new companies started with outside investor money</td>
<td>Established companies funding electronic commerce initiatives with their own capital</td>
</tr>
<tr>
<td>Connection technologies</td>
<td>Many electronic commerce participants used slow Internet connections</td>
<td>Rapidly increasing use of broadband technologies for Internet connections</td>
</tr>
<tr>
<td>E-mail contact with customers</td>
<td>Unstructured e-mail communication with customers</td>
<td>Customized e-mail strategies now integral to customer contact</td>
</tr>
<tr>
<td>Advertising and electronic commerce integration</td>
<td>Overreliance on simple forms of online advertising as main revenue source</td>
<td>Use of multiple sophisticated advertising approaches and better integration of electronic commerce with existing business processes and strategies</td>
</tr>
<tr>
<td>Distribution of digital products</td>
<td>Widespread piracy due to ineffective distribution of digital products</td>
<td>New approaches to the sale and distribution of digital products</td>
</tr>
<tr>
<td>First-mover advantage</td>
<td>Rely on first-mover advantage to ensure success in all types of markets and industries</td>
<td>Realize that first-mover advantage leads to success only for some companies in certain specific markets and industries</td>
</tr>
</tbody>
</table>
Today E-commerce is a byword in Indian society and it has become an integral part of our daily life.

There are websites providing any number of goods and services.

Then there are those, which provide a specific product along with its allied services.
SWOT Analysis of the Industry

Most of the time we see that the use of electronic techniques for doing business add value either by the reducing transaction cost or by creating some type of network effect, or by a combination of both.

In SWOT analysis (the acronym is short for Strengths, Weaknesses, Opportunities and Threats), here we try to find out the strengths and weaknesses of ecommerce in respect of Indian business environment.
<table>
<thead>
<tr>
<th>The organisation</th>
<th>Stengths – S</th>
<th>Weaknesses – W</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Existing brand</td>
<td>1. Brand perception</td>
<td></td>
</tr>
<tr>
<td>2. Existing customer base</td>
<td>2. Intermediary use</td>
<td></td>
</tr>
<tr>
<td>3. Existing distribution</td>
<td>3. Technology/skills</td>
<td></td>
</tr>
<tr>
<td>4. X-channel support</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opportunities – O</th>
<th>SO strategies</th>
<th>WO strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Cross-selling</td>
<td>Leverage strengths to maximise opportunities = Attacking strategy</td>
<td>Counter weaknesses through exploiting opportunities = Build strengths for attacking strategy</td>
</tr>
<tr>
<td>2. New markets</td>
<td>= Build strengths for offensive strategy</td>
<td></td>
</tr>
<tr>
<td>3. New services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Alliances/Co-branding</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threats – T</th>
<th>ST strategies</th>
<th>WT strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Customer choice</td>
<td>Leverage strengths to minimise threats = Defensive strategy</td>
<td>Counter weaknesses and threats = Build strengths for defensive strategy</td>
</tr>
<tr>
<td>2. New entrants</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. New competitive products</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Channel conflicts</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Introduction

Contents

- Threats
- Threats to information security
- Acts of Human Error or failure
- Espionage/Trespass
- Network Security Goals
- Some key factors for success in E-commerce
- The EC Security Environment: The Scope of the Problem
- Dimensions of E-commerce Security
- Security Threats in the E-commerce Environment
• A threat is an object, person, or other entity that represents a constant danger to an asset.
• Management must be informed of the various kinds of threats facing the organization.
• By examining each threat category, management effectively protects information through policy, education, training, and technology controls.
## Threats to information security

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Acts of human error or failure</td>
<td>Accidents, employee mistakes</td>
</tr>
<tr>
<td>2. Compromises to intellectual property</td>
<td>Piracy, copyright infringement</td>
</tr>
<tr>
<td>3. Deliberate acts of espionage or trespass</td>
<td>Unauthorized access and/or data collection</td>
</tr>
<tr>
<td>4. Deliberate acts of information extortion</td>
<td>Blackmail of information disclosure</td>
</tr>
<tr>
<td>5. Deliberate acts of sabotage or vandalism</td>
<td>Destruction of systems or information</td>
</tr>
<tr>
<td>6. Deliberate acts of theft</td>
<td>Illegal confiscation of equipment or information</td>
</tr>
<tr>
<td>7. Deliberate software attacks</td>
<td>Viruses, worms, macros, denial-of-service</td>
</tr>
<tr>
<td>8. Forces of nature</td>
<td>Fire, flood, earthquake, lightning</td>
</tr>
<tr>
<td>9. Deviations in quality of service from service providers</td>
<td>Power and WAN service issues</td>
</tr>
<tr>
<td>10. Technical hardware failures or errors</td>
<td>Equipment failure</td>
</tr>
<tr>
<td>11. Technical software failures or errors</td>
<td>Bugs, code problems, unknown loopholes</td>
</tr>
<tr>
<td>12. Technological obsolescence</td>
<td>Antiquated or outdated technologies</td>
</tr>
</tbody>
</table>
Acts of Human Error or Failure

• Include acts done with no malicious intent.
• Caused by:
   Inexperience
   Improper training
   Incorrect assumption
   Other circumstances
• Employees are greatest threats to information security - they are closest to organization data.

• Employee mistakes can easily lead to the following:
   Revealing classified data
   Entry of erroneous data
   Accidental deletion or modification of data
   Storage of data in unprotected areas
   Failure to protect information
• Many of threats can be prevented with controls.
Espionage/Trespass

- Broad category of activities that breach confidentiality
  - Unauthorized accessing of information
  - Competitive intelligence vs. espionage
  - Shoulder surfing can occur any place a person is accessing confidential information
- Controls implemented to mark the boundaries of an organization’s virtual territory giving notice to trespassers that they are encroaching on the organization’s cyberspace
- Hackers uses skill, guile, or fraud to steal the property of someone else
Network Security Goals

- **Confidentiality**: only sender, intended receiver should understand message contents
  - sender encrypts the message
  - Receiver decrypts the message
  - Privacy

- **Integrity**: sender and receiver want to make sure that the message are not altered without detection

- **Availability**: service must be available to user (instead of “Non-repudiation” in security service)

- **Authentication**: sender and receiver want to confirm the identify of each other

- **Access control**: service must be accessible to users
Some key factors for success in E-commerce

- Providing value to customers
- Providing service and performance
- Look
- Advertising
- Personal attention
- Providing a sense of community
- Providing **reliability** and **security**
- Providing a 360-degree view of the customer relationship
The EC Security Environment: The Scope of the Problem

• In 2002 Computer Security Institute survey of 503 security personnel in U.S. corporations and government
• 80% of respondents had detected breaches of computer security within last 12 months and suffered financial loss as a result
• Only 44% were willing or able to quantify loss, which totaled $456 million in aggregate
• 40% experienced denial of service attacks
• 40% reported attacks from outside the organization
• 85% detected virus attacks
Dimensions of E-commerce Security

- **Integrity** (*ability*) to ensure that information being displayed on a Web site or transmitted/received over the Internet has not been altered in any way by an unauthorized party.

- **Non-repudiation** (*ability*) to ensure that e-commerce participants do not deny (repudiate) online actions.

- **Authenticity** (*ability*) to identify the identity of a person or entity with whom you are dealing on the Internet.

- **Confidentiality** (*ability*) to ensure that messages and data are available only to those authorized to view them.

- **Privacy** (*ability*) to control use of information a customer provides about himself or herself to merchant.

- **Availability** (*ability*) to ensure that an e-commerce site continues to function as intended.
Dimensions of E-commerce Security

- Integrity
- Non-repudiation
- Confidentiality
Security Threats in the E-commerce Environment

- Three key points of vulnerability:
  - Client
  - Server
  - Communications channel

- Most common threats:
  - Malicious code
  - Hacking and cyber vandalism
  - Credit card fraud/theft
  - Spoofing
  - Denial of service attacks
  - Sniffing
  - Insider jobs
Denial Of Service (DoS)

Hacker

Unwitting Host “Zombie”

Other Network Computers

Victim’s Server

User PCs
Cryptography

Contents

• E-commerce Security Requirement
• Introduction to “Cryptography”
• Concept of Encryption and Decryption
• Encryption techniques
  ◆ Symmetric algorithm
  ◆ Asymmetric algorithm
• Message Authentication
• Cryptography-based protocols applications & solutions
E-commerce Security Requirement

- commerce over open networks (such as internet) can secure if the following happen:

1. Server Security
2. Message Privacy (or confidentiality)
3. Message integrity
4. Authentication
5. Authorization
6. Audit mechanism and non-repudiation
7. Payment and settlement
1. Server Security:

- Use **firewalls** and proxy servers
- Every packet going from the firm's computer to the internet or voice versa will be checked
- “Security” against “attack” such as **viruses**, unauthorized access of hackers, trojan horse can be provided.
2. Message Privacy
   - A key requirement for E-commerce
   - It assures that the communication between trading parties are not revealed to other, therefore unauthorized party can not read or understand the message.

3. Message integrity
   - Another key requirement for e-commerce
   - It assures that the communication between trading parties are not alerted by an enemy.
4. Authentication

- Assures that the “sender” of the message is actually the person he/she claims.
- Paper message
- The term “authentication” determines the user of the computer is actually who he/she claims.
- The term “authentication of the receiver”: allows the sender to be sure that the party he/she intend to get the message is the one who is receives it.
5. Authorization

- Ensures that the trading party has the **authority of transaction**
- It prevents the risks that employees transactions create economic damage

**Authentication vs Authorization**

- Once the system knows who the user is through authentication, Authorization is how the system decides what the user can do
6. Audit mechanism and non-repudiation
   - Enables exchanging parties to maintain and revisit the history/sequence of events during a period of transaction
   - In e-commerce, these could be computer time stamps, or records of different computer of different stage of transactions

7. Payment and settlements
   - Vital to widespread e-commerce
   - Secure e-payment ensures that “commitment” to pay for goods/services over media are met
Introduction to “Cryptography”

- Plaintext = means the message
- Encryption = encoding (hiding the contents from outsiders) the message
- Ciphertext = the encrypted message
- Decryption = the process of retrieving the plaintext from the ciphertext
- “Encryption” and “Decryption” makes use of a “key and a coding method”.
Concept of Encryption and Decryption

Sender

Encryption algorithm

Ke

Ciphertext

Network

Decryption algorithm

Kd

Plaintext

Receiver

Plaintext
Goals of Cryptography

- **Security goals:**
  - privacy (secrecy, confidentiality)
    - only the intended recipient can see the communication
  - authenticity (integrity)
    - the communication is generated by the alleged sender
• There are three important encryption techniques now in use:
  - Symmetric or “private key” encryption
  - Asymmetric or “public key” encryption
  - Digital signature, which are based on a variation of public key encryption.
Encryption techniques

Symmetric Encryption

Asymmetric Encryption
• **Data Encryption Standard (DES)** is a symmetric algorithm developed by IBM and maintained by the National Institute of Standard and Technology. It is based on encryption multiple times with different keys. A 56-bit version of DES is commonly used, but can be broken by brute force.

• Other Symmetric encryption techniques include:
  - **RC4** uses a 40 bit key, but can use up to 256 bits.
  - **Triple DES (3DES)** used DES three times, effectively giving it a 168 bit key.
  - **Advance Encryption Standard (AES)**, design to replace DES uses 128, 192, and 256 bit keys.
**Symmetric algorithm - RC4**

- **RC4 (Rivest Codes 4)** is the most widely-used software stream cipher and is used in popular protocols such as **Secure Sockets Layer (SSL)** to protect:
  - Internet traffic
  - Secure wireless networks

- Remarkable for its simplicity and speed in software
- RC4 has weaknesses that argue against its use in new systems. It is especially vulnerable when
  - The beginning of the output keystream is not discarded,
  - Nonrandom or related keys are used,
  - Or a single keystream is used twice;
3DES is a minor version of DES
Breaking 3DES is much more difficult than DES
It defines 3 keys (k1, k2, k3) of 168 bits (3 * 56 bit)
Ciphertext (C) is generated from encryption of plaintext (P) by the:
\[ C = E_{k3} \left( D_{k2} \left( E_{k1}(P) \right) \right) \]
Decryption of the ciphertext is produced by:
\[ P = D_{k1} \left( E_{k2} \left( D_{k3}(C) \right) \right) \]
Symmetric algorithm - 3DES

- Security can be increased by encryption multiple times with different keys.
- Double DES is not much more secure than single DES because of a “meet-in-the-middle” attack.
- 3DES (168 bit of keys) can be cracked by trying 112 bits of keys.
Advancing Encryption Standard (AES) characteristics:

- Private key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger & faster than triple-DES
- Provide full specification & design details
- Both C & java implementations
- NIST have released all submissions & unclassified analyses
Symmetric algorithm – AES

• Initial Criteria:
  ✓ Security- effort for practical cryptanalysis
  ✓ Cost- in term of computational efficiency
  ✓ Algorithm & Implementation characteristics

• Final Criteria:
  ✓ General security
  ✓ Ease of software & hardware Implementation
  ✓ Implementation attacks
  ✓ flexibility
• after testing and evaluation, shortlist in Aug-99:
  – MARS (IBM) - complex, fast, high security margin
  – RC6 (USA) - v. simple, v. fast, low security margin
  – Rijndael (Belgium) - clean, fast, good security margin
  – Serpent (Euro) - slow, clean, v. high security margin
  – Twofish (USA) - complex, v. fast, high security margin
• then subject to further analysis & comment
International Data Encryption algorithm (IDEA) is a 64-bit block cipher with a 128-bit key. Reputation of quality and strength. Some algorithm for both encryption and decryption (i.e. symmetric cryptography) with 8 main iteration. It is based on mixing operations from different algebraic groups (XOR, addition module 2 to the power of 16, Multiplication module 2 the power of 16 plus 1). It runs much faster than DES. The main drawback is that it is patented and requires license for all but non-commercial use.
In cryptography, an S-Box (Substitution-box) is a basic component of Symmetric key algorithms which performs substitution.

In block ciphers, they are typically used to obscure the relationship between the key and the ciphertext.

In many cases, the S-Box are carefully chosen to resist cryptanalysis.

In general, an S-Box takes some number of input bits, $m$, and transforms them into some number of output bits, $n$: an $m \times n$ S-box can be implemented as a lookup table with $2^m$ words of $n$ bit each.

Fixed tables are normally used, as in the (DES), but in some cipher the tables are generated dynamically from the key.
<table>
<thead>
<tr>
<th></th>
<th>DES</th>
<th>DES vs AES</th>
<th>AES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Date</strong></td>
<td>1976</td>
<td>1999</td>
<td></td>
</tr>
<tr>
<td><strong>Block size</strong></td>
<td>64</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td><strong>Key length</strong></td>
<td>56</td>
<td>128, 192, 256</td>
<td></td>
</tr>
<tr>
<td><strong>Number of rounds</strong></td>
<td>16</td>
<td>9, 11, 13</td>
<td></td>
</tr>
<tr>
<td><strong>Encryption primitives</strong></td>
<td>Substitution, permutation</td>
<td>Substitution, shift, bit mixing</td>
<td></td>
</tr>
<tr>
<td><strong>Cryptographic primitives</strong></td>
<td>Confusion, diffusion</td>
<td>Confusion, diffusion</td>
<td></td>
</tr>
<tr>
<td><strong>Design</strong></td>
<td>Open</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td><strong>Design rationale</strong></td>
<td>Closed</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td><strong>Selection process</strong></td>
<td>Secret</td>
<td>Secret, but accept open public comment</td>
<td></td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>IBM, enhanced by NSA</td>
<td>Independent cryptographers</td>
<td></td>
</tr>
</tbody>
</table>
- The second type of key-based algorithms:
  - Use different key for decryption (or the decryption key cannot be derived from encryption key)
  - Permits the encryption key to be public(anyone can encrypt with the sites public key), whereas only the right recipient or site can decrypt the message.
  - The encryption key is also called public key and the decryption key is called secret key or private key.
Public-key cryptosystem-authentication mode
Public-key cryptosystem - encryption mode

A’s Public Key

A’s Secret Key
• While many public key cryptographic systems introduced so far only the following three proved to be secure and efficient:
  ✦ Integer factorization systems (e.g. RSA)
  ✦ Logarithm System (e.g. Digital Signature Algorithm or DSA)
  ✦ Elliptic curve cryptosystem (also defined as the elliptic curve discrete logarithm system.)
Message Authentication

• Protection against active attacks
  ★ Falsification of data
  ★ Eavesdropping

• Message is authentic if it genuine and comes from the alleged source.

• Authentication allows received to verify that message is authentic
  ★ Message has not altered
  ★ Message is from authentic source
  ★ Message timeline
• Assumes sender and receiver are only entities that know key
• Message includes:
  - Error detection code
  - Time stamp
  - Sequence number
• Generate authentication code based on shared key and message
• Command key shared between A and B
• If only sender and receiver know key and code matches:
  ✴ Receiver assured message has not altered
  ✴ Receiver assured message is from alleged sender
  ✴ If message has sequence number, receiver assured of proper sequence
• Authentication tag generated and appended to each message
• Message not encrypted
• Useful for:
  ➢ One side heavily loaded
    ▪ Encryption adds to worked
    ▪ Can authentication random message
  ➢ Message broadcast to multiple destinations
    ▪ Have one destination responsible for authentication
  ➢ Program authentication without encryption and can be executed (without decoding)
Message Authentication Using Message Authentication Code
Cryptography-based protocols, applications & solutions

- Secure Socket Layer (SSL/TLS)
- Digital Signatures
- Digital Certificates
- Secure Electronic Transaction (SET)
- Authentication POP (APOP)
- Pretty Good Privacy (PGP/GPG)
- Kerberos
- Secure shell (SSH)
Pretty Good Privacy (PGP/GPG)

- An application for encryption, digitally signing, decryption, and verifying the integrity and authenticity of messages.
- Allows user to encrypt/decrypt **whole message** using a variety of public key encryption algorithms.
- Allow user to **create** and **verify** digital signatures.
- Now available, in a variety of ports and re-writes, for all popular operating systems.
• A network authentication protocol, developed by MIT.
• Designed to provide strong authentication in multi-server, multi-client environments, using symmetric (secret-key) encryption.
• Available in commercial and Open Source implementations.
• Provides both secure authentication and (optional) encryption of all communications.
• Based on a centralised Authentication Server.
• Kerberos version 5 has been proposed as an internet standard.
Pop is “Post Office Protocol”, a standard Internet protocol for downloading received email on a mail server to workstation’s mail reader.

- Pop
  - Send user ID and password over network as plain text
  - Almost universal

- APOP
  - Encrypts password
  - Used MD5 algorithm
  - Only available to mail client that support APOP
Secure Electronic Transaction (SET)

- An open encryption and security specification for **protecting payment card transaction** on the internet

- Feature:
  1) Protects **privacy** of transmitted payment and ordering
  2) Ensures **integrity** of all transmitted data
  3) Provides **authentication** that a payment card holder is a legitimate
  4) Allows payment card holder to **verify that the merchant has a relationship whit an institution that allow it to accept payment cards**.

- Implemented by large e-commerce vendors for large financial institutions....
  - E.g., Verifone supplied SET to the Royal Bank of Canada
1. **Customer** opens account with a bank that support e-payment and SET.
2. **Customer** receives her own X.509 digital certificate, signed by the bank.
3. **Merchants** maintain their own X.509 digital certificates.
4. **Customer** places e-commerce order identifying items and total.
5. **Merchant** sends his certificate for verification by customer.
6. **Payment info** (and customer’s certificate) send by customer.
7. **Merchant** requests credit authorisation from bank.
8. **Merchant** confirms order to customer.
9. **Merchant** provides goods/services.
10. **Merchant** requests payment from bank.
• An electronic and Digital Signatures
  - Authenticates the identity of the sender of a message, or the signer of a document,
  - Or ensures that the contents of a message are intact.

• Digital Signatures features:
  - Are easily transportable,
  - Cannot be imitated by someone else,
  - And can be automatically time-stamped.

• The ability to ensure that the original signed message arrived means that:
  • the sender can not easily repudiate it later.
Digital Signatures

• Encryption
  o Symmetric Systems – same key to encrypt & decrypt-DES
  o Asymmetric System- also known as **public key encryption**
  o Different key to decrypt-RSA
  o Digital Signatures- utilise the public key of organizations
Digital Signatures

- Sender **encrypts** message with their **private key**
- Receiver can **decrypt** using **sender public key**
- The **authenticates sender**, who is only person who has the matching key.
- Does not give “privacy” of data
  - decrypt key is public
Digital Signatures are a cryptographic technique and are one of the most important application of asymmetric public-key cryptography.

They are electronic or digital signature that can be used to **authentication** the identity of the sender of the message or the signer of the document (to ensure that content of the sent message unchange).

A “Signature” is a pair of functions (Sig, Ver) of a key pair and a bit stream M.
The Digital Signature, is a small part of message, and includes:

- The name of the sender
- Other key contents

The Digital Signature in the outgoing message is encrypted using the sender’s private key.

The Digital Signature is then decrypted using the sender’s public key thus providing evidence that the message originate from the sender.

Digital Signature and public key encryption combine to provide secure and authentication message transmission.
Digital Signatures - How?

• sender
  1. Create a message
  2. Hash the message to product a message digest
  3. Encryption the message digest with sender’s private key
  4. Append the encrypted digest to the message
  5. Send message

• recipient
  1. Receive message
  2. Decrypt the message digest whit the sender’s public key
  3. If this work’s the sender is authenticated
  4. Hash the message to produce another message digest
  5. Compare message digest in step 2 with step 4. if the same, the message has been changed.
Digital Signatures

Sender

Message

To be, or not to be, that is the question, whether tis nobler in the...

Message Digest

Message Digest Algorithm

Sender's Private Key

Encryption Algorithm

Message Digest

Receiver

Message

To be, or not to be, that is the question, whether tis nobler in the...

Message Digest

Message Digest Algorithm

Sender's Public Key

Encryption Algorithm

Message Digest

Message transmitted correctly

equal? yes

no Error! Message has been modified!
- Diffe-Hellman
  - Oldest public key cryptography system still in use
  - Intended to allow sender and recipient to share a secret key
- E1 Gamal
  - Signature scheme base on Diffe-Hellman
- DSA (Digital Signature Algorithm)
  - Based on E1 Gamal
  - Primarily performance improvements, eg. for smart cards
- SHA (Secure Hash Algorithm)
- MD5 (Message Digest 5)
  - Create message digest of fixed length
Some Type of Digital Signatures

1. Blind Digital Signature Schemes
2. Undeniable Signature Schemes
3. Fail-stop Signature Schemes
4. Proxy Signature Schemes
5. Group Signature Schemes
E D I
a new business paradigm
Components

- Definitions
- Strategic Importance Initial
- Benefits of EDI
- Technical Aspects of EDI
- Standardisation
- Legal Aspects of EDI
- Implementation
- Summary
• **Electronic Commerce (EC)**
  
  is the paperless exchange of business information, using Electronic Data Interchange (EDI), electronic mail, electronic bulletin boards, electronic funds transfer and other similar technologies.
Electronic Data Interchange (EDI)

- a major part of Electronic Commerce (EC), is the computer-to-computer exchange of business data in a standard, machine-processable format. The information is generally patterned after a conventional paper document, such as a purchase order or invoice. It is a “paperless trading”
• Trading Partner

  - A trading partner is any company, government department, or commercial or non-commercial entity with whom an organization regularly exchanges documents of formatted data (not just letters or memos).
Trading Partner Agreement

- A signed document between trading partners outlining all the conditions that will allow electronic communication. The agreement states that the parties intend to be legally bound in the same manner as though they were exchanging paper documents. The signature on the agreement serves as a substitute for signatures on paper documents.
Definitions

• **Mapping**
  – The process of taking data from a company-specific format and fitting it into the EDI standard electronic format (as defined by a particular transaction set).

• **Transaction Set**
  – An EDI standard electronic format for a business document.
Definitions

• Translation Software
  – Software used to take information from a flat data file and convert it into an EDI standard electronic format.
• Value Added Network (VAN)
  – A third party network performing services beyond the transmission of data. For example, VANs provide mailbox, data security, and data archiving services. Many also offer e-mail services.
**VAN Interconnection**

- The connection between two VANS that allows messages from one VAN’s customers to be communicated to the customers on the other.
Strategic Importance Initial

• Time

  – Through the use of EDI, companies are able to improve their response time and decrease their time to market by accelerating the Purchase Order-to-Invoice-to-Payment process from weeks or days to hours, or even minutes. Not only were they shorter, but they were also more accurate and reliable.
• **Service**
  – Another benefit of these changes was the improvement in customer service levels.

• **Market**
  – Companies could then use these advantages to respond more quickly to new entrants in the market.
Costs benefits

Through the use of EDI, innovative business programs such as Just-In-Time inventory management were possible. EDI and JIT allowed companies to have more control over their inventory levels and reduce their costs by increasing inventory turns and decreasing safety stocks.
Benefits of EDI

• Transactions speed
  – has greatly increased with the creation of EDI.
  – EDI drastically reduces this problem by sending transactions electronically where they can be sent and received almost simultaneously.
Benefits of EDI

• Direct transmission

  – EDI includes the direct transmission of data between organizations VAN. EDI is not facsimile transmission (fax) of information nor is it electronic mail (e-mail). Both of these transmission types are in “free format” (not standard format) and, therefore, generally require rekeying of data into the receiver’s computer system.
Benefits of EDI

• **Cut down the possibility of human error**
  
  – EDI would also cut down on the tendency for "human error". EDI eliminates this possibility because the receiving end is a computer that simply translates the message that has already been keyed into the system.
Benefits of EDI

- Reduces the risk of lost data
  - whether that means the data is physically unable to be located, or if only part of the data has been lost through the numerous steps required to conduct business through the use of paper.
Benefits of EDI

• The benefits of EDI include:
  – Time savings and associated financial savings accrued,
  – Improved accuracy,
  – Improved trading partner relationships and client interactions,
  – Improved reconciliation of transactions exchanged.
Technical Aspects of EDI

- EDI messages
  - EDI messages are passed through a Value Added Network or "VAN." In principle a VAN is an electronic mail station for holding and passing messages.
Technical Aspects of EDI

• Services for a VAN would include:
  – Storing and forwarding messages
  – Communications between standard data formats
  – Detecting and correcting errors
  – Message decryption and encryption
Technical Aspects of EDI

• EDI Hardware
  EDI transactions can be passed from many types of computers (i.e. PC, Mac, UNIX, and mainframe). Trading partners do not need to use the same type of equipment. EDI messages are hardware independent, due in part to the X12 standard. The transactions are sent via dedicated links, ISDN or phone lines.
Technical Aspects of EDI

• EDI software
  – **Translation software** takes raw data and arranges it into the X12 format or the United Nations EDIFACT standard on the sender's end.
  – **Mapping software** is used to exchange information between the company's EDI transactions and its other internal applications such as inventory, accounts receivable, and accounting and ordering.
• **Communicating EDI transactions**
  
  – can be done in several ways. The data can be transmitted and received via a dedicated computer system using async, bi-sync, X25, X.400, Internet or other telecommunication standards and networks. Depending on the size of the company and number of trading partners, these methods can occur in combination with one another or by themselves.
• ANSI ASC X12

- EDI standard in North America and the reference standard. The X12 committee is charged with developing "standards to facilitate electronic interchange relating to order placement and processing, shipment and receiving information, invoicing, payment, and cash application data"
• **UN/EDIFACT**

– the ANSI X12 standards and the European standards, known as "Guidelines for Trade Data Interchange" (GTDI). Immediately prior to the formulation of EDIFACT, European EDI standards had undergone a process of reconstruction by the United Nations Economic Commission for Europe (UNECE)
Legal Aspects of EDI

• Authenticity
  – Determining the authenticity of information transmitted electronically (genuine; true; real; pure; reliable; trustworthy; having the character and authority of an original; ...competent, credible, and reliable as evidence).
Legal Aspects of EDI

• Written Requirement
  – A number of laws require that certain legal documents, such as contracts, wills, and commercial paper be written on paper and signed.
Legal Aspects of EDI

• **Existing Laws**

  – it is clear that something needs to be done to clarify the laws with regard to EDI at this time and especially in the near future.
Legal Aspects of EDI

• Privacy
  – Privacy and security issues must be determined at the outset of an EDI relationship, preferably in the trade agreement.
Implementation

• It’s a general idea if EDI can and should be implemented into your processes.
  – 1. Identify EDI Opportunities
  – 2. Cost-Effectiveness Analysis & Approval
    • 2.1. Estimate Benefits.
    • 2.2. Estimate Investment Costs.
    • 2.3. Estimating Operating Costs.
    • 2.4. Estimate Net Benefits, net costs.
    • 2.5. Establishing EDI Priorities.
ADVANTAGES OF E-COMMERCE

› Faster buying/selling procedure, as well as easy to find products.
› Buying/selling 24/7.
› More reach to customers, there is no geographic limitations.
› Low operational costs and better quality of services.
› No need of physical company set-ups.
› Easy to start and manage a business.
› Customers can easily select products from different providers.
ADVANTAGES OF E-COMMERCE

› Lots of Choices
› Easier to Compare Prices
› No Need to Handle Currency Notes
› Eliminate Travel Time and Cost
› E-commerce helps organization to provide better customer services.
DISADVANTAGES OF E-COMMERCE

› Unable to examine products personally
› Not everyone is connected to the Internet
› There is the possibility of credit card number theft

:Security:
› Lack of Personal Touch
› Delay in Receiving Goods
Future of ecommerce in India
Quick Stats:

Why Consumer Prefer Shopping Online?
Simple, easy, quick and limited traveling.

80% of Internet users prefer to buy online for the following main reasons:

- **73%** Time Saving
- **54%** Less Prices
- **50%** More Variety
- **42%** Less Taxes
- **28%** No Crowd
Quick Stats:

- Rising living standards
- Increased awareness
- Greater wireless internet access through mobiles
- Lack of good offline retail channels
- Improving online availability
- New payment options
e-Commerce Sales (in Cr.)

Year | Sales (Cr.)
-----|------------
2009 | ₹ 16,600
2010 | ₹ 21,700
2011 | ₹ 28,500
2012 | ₹ 40,300
2013 | ₹ 55,600
2014 | ₹ 77,100
2015 | ₹ 107,600
Quick Stats:

Mobile E-Commerce
The most used platforms are hand held devices today.

$1 Trillion
Expected Mobile transactions by 2015

Asia/Pacific would be expected to top the list.

- 94% of the smartphone users access internet with phones in India.
- 87% of the smart phone users compare prices online in India.
- 70% smart phone users access online shopping websites in India.
Quick Stats:

Mobile eCommerce Today

Anytime Access
Gives you the flexibility of reaching anywhere by the user.

Browser or App
App allows more closer reach of the users.

Large User-base
Mobile user base is adding up to 9 million connections a month.

As you know time had been the most important factor in Ecommerce

Android and iOS had been two majorly used platform today.

90% of the users use mobile phones for the day today activities.
E - Payment
Forms of E-Payment System

1. Online Credit Card Transaction System
2. Digital Cash
3. Online Stored Value System
4. Digital Accumulating Balance Payment System
5. Digital Credit Account
6. Digital Checking
1. **Online Credit Card Transaction System**

- Works on mutual trust between consumer and merchant
- Merchants never see the actual card (card not present transaction)
- No card impression is taken
- No signature is available
- Charges can be disputed later by consumer
- Merchant faces risk of transaction being disallowed in case of dispute
Parties Involved

- Consumer
- Merchant
- Clearing House
- Merchant’s Bank (Acquiring Bank)
- Consumer’s Credit Card Issuing Bank
Online Credit Card Transaction

1. Customer makes purchase

2. Secure connection through Internet to merchant

3. Merchant software contacts clearing house

4. Clearinghouse verifies account & balance with issuing bank

5. Issuing bank credits merchant account

6. Monthly statement issued with debit for purchase
Credit Card E-commerce Enablers (Internet Payment Service Provider)

- Provides merchant a secure merchant account
- Provides payment processing software installed on merchant’s site
- Collects transaction information from merchant’s site
- Routes the transaction via VeriSign (Internet security service provider) payment gateway to appropriate bank
- Ensures a customer authorized to make purchase
- Funds transferred to merchant account
Limitation of Online Credit Card Payment System

- merchant’s risk
- additional cost for merchant 3.5% appx. + transaction cost
- security risk for consumer’s credit card
- neither merchant nor consumer authenticated
- all customers cannot afford credit card
- not suited for transactions of small amounts
Security Methods

- Secure Socket Layer (SSL)
- Secure Electronic Transaction (SET)
- Digital Wallet
SSL automatically encrypts data passing between consumer’s Web browser and a merchant’s server.
Secure Electronic Transaction Protocol

SET software encrypts a digital envelope of digital certificates specifying the payment details for each transaction. SET is expected to become the dominant standard for secure electronic payments on the Internet.

• open standard for E-Commerce industry
• developed & offered by Master Card & Visa
• facilitates and encourage improved security for credit card transactions
1. Consumer makes purchase selects SET payment option

2. Merchant & consumer computers verify each other’s identity SET encrypts order & payment information

3. Merchant software forwards encrypted message

4. Clearinghouse verifies account & balance with issuing bank

5. Issuing bank credits merchant account

6. Monthly statement issued with debit for purchase
• authenticate Credit Card holders
• authenticate Merchant’s identity
• uses digital signature to verify sender’s identity
• credit card company issues digital certificate to card holder
• digital certificate stored in digital wallets
• merchant issued digital certificate by bank providing merchant account
Digital wallet authenticates the consumer through the use of digital certificates or other encryption methods, stores and transfers value, and secure the payment process from the consumer to the merchant.

**Authentication**

Confirms identities via Digital certificates, SET, or other forms of encryption.
Processing of Payments

Pays bills via alliances with credit card associations & banks.

Privacy

Customers controls their digital environment by using PIN, Card No. & Password.

Receipt Management

Reviews all transactions at a single source

Payment Management

Presents & pays bill at a single location.

Micro Payments

Makes payment under $5 anywhere on the web based on credit cards.
## Types of Digital Wallets

<table>
<thead>
<tr>
<th>Client Based Wallets</th>
<th>Server Based Wallets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gator</td>
<td>Microsoft Passport</td>
</tr>
<tr>
<td>Master Card wallet</td>
<td>Cybercash InstaBuy</td>
</tr>
<tr>
<td></td>
<td>Novell DigitalMe</td>
</tr>
<tr>
<td></td>
<td>Yodlee</td>
</tr>
</tbody>
</table>
Client Based Wallets

- software application installed on consumer’s computer
- automatically fills forms at Online stores
- merchant install software to receive client based wallet information
- when consumer clicks merchant’s site merchant queries consumer’s digital wallet
- more difficult to update as download required merchant’s form changes
Server based Wallets

• No special software for consumer required
• Financial Institutions market the system to merchants as part of their financial service package
• Technology services (infrastructure for processing payments) & Wallet services provided.
• Easy & secure shopping using whichever payment method consumer desires
• Lower transaction cost
• Lower consumer acquisition & retention costs
• Dynamically updates as merchants form change
• Consumer provided with Single Sign-In Service (SSI)
A consumer can obtain a Passport by opening an E-Mail account at MSN or Hotmail or registering at passport.com.

To obtain a unique sign-in-profile the user submits a sign in login name, password and general background information.

This information is encrypted using SSL.

The user has an option of creating a wallet profile containing credit card payment information.

The user is issued a 64 bit Passport Unique Identifier (PUID).

This PUID is sent to the merchant when the user login at the Microsoft passport login of the merchant site.

The actual password is not sent to the merchant.
Microsoft Passport Wallet

Passport

Passport Login Server

Passport user's Browser

Internet

Participating Site

Web Server

Passport Manager

Web Page

1. Web Server sends a request to Passport Manager.
2. Passport Manager retrieves the Passport user's credentials.
3. Passport Manager sends the credentials to the Passport user's Browser.
4. The Passport user's Browser verifies the credentials.
5. The Passport user's Browser sends the verified credentials to the Participating Site.
6. The Participating Site uses the credentials to access the user's data.
The registered consumer clicks the Passport logo at the merchant’s site

1 The consumer enters the Passport sign in name and password in the Passport sign in page

2 & 3 The Sign in Page is redirected to Microsoft Passport server to authenticate the consumer

The Passport authenticates the consumer & writes a cookie to the consumer’s browser containing encrypted authentication and passport profile information

4 & 5 The passport manager at the merchant’s site decrypts the information

6 The Passport Manager then caches the user ‘s authentication and profile information in the cookie on the consumer’s browser & reverifies it
2. Digital Cash (e-cash)
• digital form of value storage & value exchange
• limited convertibility into other forms of value
• require intermediaries to convert.
• used for sending small amount of money over the net
• Examples B to C
  DigiCash now e-Cash
  Millicent
  Peer to Peer
  Paypal
  Yahoo Paydirect
  MoneyZap
1. Establish account at Bank
2. Downloads Digital Wallet With private & public key
3. Sends request for e-cash coins
4. 
5. Spend e-cash
6. Merchant transfers e-cash coins back to the bank
7. Bank credits merchant’s account at bank
3. Online Stored Value System

• Instant online payment

• Value stored in an online account

• A digital wallet downloaded or money transferred from credit card account into online stored value account

**Example:** Ecount

Pre paid debit account

It is treated as if it is a MasterCard

Recipient must sign up with Ecount to access payment
1. Establish account at Ecount, funded by credit or Debit Card
2. Verify account & balance
3. Make purchase from merchant or individual by choosing MasterCard option or cash via E-mail
4. Ecount transfers funds to merchant or individual
5. Monthly statement issued to consumer showing debit to Ecount

SSL secure encrypted connection
4. Digital Accumulating Balance Payment System

- used for making micro payments
- accumulates debit balance
- billed at the end of the month
- ideal for purchasing intellectual property from Net

Example: qPass

iPIN

Millicent
Digital Credit Card Payment System

- extends functionality of existing Credit Card Systems
- safer than traditional Credit Card
- authenticates both parties by verifying digital certificates
- automatic form completion
- credit card bills paid at month end by credit or debit account or a bank account
1. Consumer signs up for eChange account
2. eChange approves application downloads digital wallet to consumer’s computer
3. Consumer uses eCharge at participating merchant
4. Authenticate merchant & consumer
5. Verify account & balances
6. Monthly statements issued showing debit to eCharge
Digital Checking

- extends functionality of an existing checking account
- Account information not revealed
- less expensive (almost half) for merchants than credit cards
- faster than paper based checking system

Examples:
- Peer to Peer
- Achex
- B to C
- Echecks
- BillPoint Electronic checks (used only at eBay)
3 b. Merchant authenticates issuing bank
THANK YOU