UNIT - III

3 E-Commerce Security and Payment Systems

Syllabus	*3.1- E-Commerce Security Environment.* *3.2- Security threats in E-Commerce* *3.3- Technology Solutions: Encryption, Securing Channels of Communication, Protecting Networks, Protecting Servers, and Clients* *3.4-Payment Systems.*

What is E-Commerce security?

e-Commerce security is the guideline that ensures safe transactions through the internet. It consists of protocols that safeguard people who engage in online selling and buying goods and services.

DIMENSIONS OF E-COMMERCE SECURITY

There are six key dimensions to e-commerce security:

1. **Integrity**
2. **Nonrepudiation**
3. **Authenticity**
4. **Confidentiality**
5. **Privacy**
6. **Availability**

ಘಟಕ - III

೩ ಇ-ಕಾಮರ್ಸ್ ಭದ್ರತೆ ಮತ್ತು ಪಾವತಿ ವ್ಯವಸ್ಥೆಗಳು

ಪಠ್ಯಕ್ರಮ	*3.1- ಇ-ಕಾಮರ್ಸ್ ಭದ್ರತಾ ಪರಿಸರ.* *3.2- ಇ-ಕಾಮರ್ಸ್‌ನಲ್ಲಿ ಭದ್ರತಾ ಬೆದರಿಕೆಗಳು* *3.3- ತಂತ್ರಜ್ಞಾನ ಪರಿಹಾರಗಳು: ಎನ್‌ಕ್ರಿಪ್ಶನ್, ಸಂವಹನದ ಚಾನಲ್‌ಗಳನ್ನು ಭದ್ರಪಡಿಸುವುದು, ನೆಟ್‌ವರ್ಕ್‌ಗಳನ್ನು ರಕ್ಷಿಸುವುದು, ಸರ್ವರ್‌ಗಳು ಮತ್ತು ಗ್ರಾಹಕರನ್ನು ರಕ್ಷಿಸುವುದು* *3.4-ಪಾವತಿ ವ್ಯವಸ್ಥೆಗಳು.*

ಇ-ಕಾಮರ್ಸ್ ಭದ್ರತೆ ಎಂದರೇನು?

ಇ-ಕಾಮರ್ಸ್ ಭದ್ರತೆಯು ಅಂತರ್ಜಾಲದ ಮೂಲಕ ಸುರಕ್ಷಿತ ವಹಿವಾಟುಗಳನ್ನು ಖಚಿತಪಡಿಸುವ ಮಾರ್ಗದರ್ಶಿಯಾಗಿದೆ. ಇದು ಸರಕು ಮತ್ತು ಸೇವೆಗಳ ಆನ್ ಲೈನ್ ಮಾರಾಟ ಮತ್ತು ಖರೀದಿಯಲ್ಲಿ ತೊಡಗಿರುವ ಜನರನ್ನು ರಕ್ಷಿಸುವ ಪ್ರೋಟೋಕಾಲ್ ಗಳನ್ನು ಒಳಗೊಂಡಿದೆ.

ಇ-ಕಾಮರ್ಸ್ ಭದ್ರತೆಯ ಆಯಾಮಗಳು

ಇ-ಕಾಮರ್ಸ್ ಭದ್ರತೆಗೆ ಆರು ಪ್ರಮುಖ ಆಯಾಮಗಳಿವೆ:

1. ಸಮಗ್ರತೆ
2. ನಿರಾಕರಣೆ
3. ಸತ್ಯಾಸತ್ಯತೆ
4. ಗೌಪ್ಯತೆ
5. ಗೌಪ್ಯತೆ
6. ಲಭ್ಯತೆ

SECURITY THREATS IN THE E-COMMERCE

From a technology perspective, there are three key points of vulnerability when dealing with e-commerce: the client, the server, and the communications pipeline.

we describe a number of the most common and most damaging forms of security threats to e-commerce consumers and site operators: malicious code, potentially unwanted programs, phishing, hacking and cybervandalism, credit card fraud/theft, spoofing, pharming, spam (junk) Web sites (link farms), identity fraud, Denial of Service(DoS) and DDoS attacks, sniffing, insider attacks, poorly designed server and client software, social network security issues, mobile platform security issues, and finally, cloud security issues.

1. MALICIOUS CODE

Malicious code (sometimes referred to as “malware”) includes a variety of threats such as viruses, worms, Trojan horses, ransomware, and bots. Some malicious code, sometimes referred to as an exploit, is designed to take advantage of software vulnerabilities in a computer’s operating system, Web browser, applications, or other software components.

a. Virus

A **virus** is a computer program that has the ability to replicate or make copies of itself, and spread to other files. In addition to the ability to replicate, most computer viruses deliver a “payload.” The payload may be relatively benign, such as the display of a message or image, or it may be highly destructive-destroying files, reformatting the computer’s hard drive, or causing programs to run improperly.

Antivirus: Antivirus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.

Example: McAfee, Norton, Bitdefender.

ಇ-ಕಾಮರ್ಸ್‌ನಲ್ಲಿ ಭದ್ರತಾ ಬೆದರಿಕೆಗಳು

ತಂತ್ರಜ್ಞಾನದ ದೃಷ್ಟಿಕೋನದಿಂದ, ಇ-ಕಾಮರ್ಸ್‌ನೊಂದಿಗೆ ವ್ಯವಹರಿಸುವಾಗ ದುರ್ಬಲತೆಯ ಮೂರು ಪ್ರಮುಖ ಅಂಶಗಳಿವೆ: ಕ್ಲೈಂಟ್, ಸರ್ವರ್ ಮತ್ತು ಸಂವಹನ ಪೈಪ್‌ಲೈನ್.

ಇ-ಕಾಮರ್ಸ್ ಗ್ರಾಹಕರು ಮತ್ತು ಸೈಟ್ ಆಪರೇಟರ್‌ಗಳಿಗೆ ಭದ್ರತಾ ಬೆದರಿಕೆಗಳ ಹಲವಾರು ಸಾಮಾನ್ಯ ಮತ್ತು ಅತ್ಯಂತ ಹಾನಿಕಾರಕ ರೂಪಗಳನ್ನು ನಾವು ವಿವರಿಸುತ್ತೇವೆ: ದುರುದ್ದೇಶಪೂರಿತ ಕೋಡ್, ಸಂಭಾವ್ಯ ಅನಗತ್ಯ ಕಾರ್ಯಕ್ರಮಗಳು, ಫಿಶಿಂಗ್, ಹ್ಯಾಕಿಂಗ್ ಮತ್ತು ಸೈಬರ್‌ವಾಂಡಲಿಸಂ, ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಂಚನೆ/ಕಳ್ಳತನ, ವಂಚನೆ, ಫಾರ್ಮಿಂಗ್, ಸ್ಪ್ಯಾಮ್ (ಜಂಕ್) ವೆಬ್‌ಸೈಟ್‌ಗಳು (ಲಿಂಕ್ ಫಾರ್ಮ್‌ಗಳು), ಗುರುತಿನ ವಂಚನೆ, ಸೇವೆಯ ನಿರಾಕರಣೆ (DoS) ಮತ್ತು DDoS ದಾಳಿಗಳು, ಸ್ನಿಫಿಂಗ್, ಒಳಗಿನ ದಾಳಿಗಳು, ಕಳಪೆಯಾಗಿ ವಿನ್ಯಾಸಗೊಳಿಸಲಾದ ಸರ್ವರ್ ಮತ್ತು ಕ್ಲೈಂಟ್ ಸಾಫ್ಟ್‌ವೇರ್, ಸಾಮಾಜಿಕ ನೆಟ್‌ವರ್ಕ್ ಭದ್ರತಾ ಸಮಸ್ಯೆಗಳು, ಮೊಬೈಲ್ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್ ಭದ್ರತಾ ಸಮಸ್ಯೆಗಳು ಮತ್ತು ಅಂತಿಮವಾಗಿ, ಕ್ಲೌಡ್ ಭದ್ರತೆ ಸಮಸ್ಯೆಗಳು.

1. ದುರುದ್ದೇಶಪೂರಿತ ಕೋಡ್

ದುರುದ್ದೇಶಪೂರಿತ ಕೋಡ್ (ಕೆಲವೊಮ್ಮೆ "ಮಾಲ್‌ವೇರ್" ಎಂದು ಉಲ್ಲೇಖಿಸಲಾಗುತ್ತದೆ) ವೈರಸ್‌ಗಳು, ವರ್ಮ್‌ಗಳು, ಟ್ರೋಜನ್ ಹಾರ್ಸ್‌ಗಳು, ransomware ಮತ್ತು ಬಾಟ್‌ಗಳಂತಹ ವಿವಿಧ ಬೆದರಿಕೆಗಳನ್ನು ಒಳಗೊಂಡಿದೆ. ಕೆಲವು ದುರುದ್ದೇಶಪೂರಿತ ಕೋಡ್ ಅನ್ನು ಕೆಲವೊಮ್ಮೆ ಶೋಷಣೆ ಎಂದು ಕರೆಯಲಾಗುತ್ತದೆ, ಕಂಪ್ಯೂಟರ್‌ನ ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್, ವೆಬ್ ಬ್ರೌಸರ್, ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಅಥವಾ ಇತರ ಸಾಫ್ಟ್‌ವೇರ್ ಘಟಕಗಳಲ್ಲಿನ ಸಾಫ್ಟ್‌ವೇರ್ ದೋಷಗಳ ಲಾಭವನ್ನು ಪಡೆಯಲು ವಿನ್ಯಾಸಗೊಳಿಸಲಾಗಿದೆ.

A. ವೈರಸ್

ವೈರಸ್ ಎನ್ನುವುದು ಕಂಪ್ಯೂಟರ್ ಪ್ರೋಗ್ರಾಂ ಆಗಿದ್ದು ಅದು ಸ್ವತಃ ಪುನರಾವರ್ತಿಸುವ ಅಥವಾ ನಕಲು ಮಾಡುವ ಸಾಮರ್ಥ್ಯವನ್ನು ಹೊಂದಿದೆ ಮತ್ತು ಇತರ ಫೈಲ್‌ಗಳಿಗೆ ಹರಡುತ್ತದೆ. ಪುನರಾವರ್ತಿಸುವ ಸಾಮರ್ಥ್ಯದ ಜೊತೆಗೆ, ಹೆಚ್ಚಿನ ಕಂಪ್ಯೂಟರ್ ವೈರಸ್ಗಳು "ಪೇಲೋಡ್" ಅನ್ನು ತಲುಪಿಸುತ್ತವೆ. ಸಂದೇಶ ಅಥವಾ ಚಿತ್ರದ ಪ್ರದರ್ಶನದಂತಹ ಪೇಲೋಡ್ ತುಲನಾತ್ಮಕವಾಗಿ ಸೌಮ್ಯವಾಗಿರಬಹುದು, ಅಥವಾ ಇದು ಹೆಚ್ಚು ವಿನಾಶಕಾರಿ-ನಾಶಗೊಳಿಸುವ ಫೈಲ್‌ಗಳು, ಕಂಪ್ಯೂಟರ್‌ನ ಹಾರ್ಡ್ ಡ್ರೈವ್ ಅನ್ನು ಮರು ಫಾರ್ಮ್ಯಾಟ್ ಮಾಡುವುದು ಅಥವಾ ಪ್ರೋಗ್ರಾಂಗಳು ಸರಿಯಾಗಿ ರನ್ ಆಗಲು ಕಾರಣವಾಗಬಹುದು.

ಆಂಟಿವೈರಸ್ ಸಾಫ್ಟ್‌ವೇರ್ ಎನ್ನುವುದು ಸಾಫ್ಟ್‌ವೇರ್ ವೈರಸ್‌ಗಳು ಮತ್ತು ವರ್ಮ್‌ಗಳು, ಟ್ರೋಜನ್‌ಗಳು, ಆಡ್‌ವೇರ್ ಮತ್ತು ಹೆಚ್ಚಿನವುಗಳಂತಹ ಇತರ ದುರುದ್ದೇಶಪೂರಿತ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ತಡೆಗಟ್ಟಲು, ಹುಡುಕಲು, ಪತ್ತೆಹಚ್ಚಲು ಮತ್ತು ತೆಗೆದುಹಾಕಲು ವಿನ್ಯಾಸಗೊಳಿಸಲಾದ ಪ್ರೋಗ್ರಾಂ ಅಥವಾ ಪ್ರೋಗ್ರಾಂಗಳ ಸೆಟ್ ಆಗಿದೆ.

ಉದಾಹರಣೆ: McAfee, Norton, Bitdefender.

B. Worm

A computer worm is a type of malware whose primary function is to self-replicate and infect other computers while remaining active on infected systems.

C. Ransomware

Ransomware (scareware) is a type of malware (often a worm) that locks your computer or files to stop you from accessing them.

D. Trojan horse

Trojan horse appears to be benign, but then does something other than expected. Often a way for viruses or other malicious code to be introduced into a computer system.

2. potentially unwanted program (PUP):

program that installs itself on a computer, typically without the user's informed consent.

A. Adware

Adware is typically used to call for pop-up ads to display when the user visits certain sites. While annoying, Adware is not typically used for criminal activities.

B. Spyware

spyware a program used to obtain information such as a user's keystrokes, e-mail, instant messages, and so on.

3. Phishing:

Any deceptive, online attempt by a third party to obtain confidential information for financial gain.

4.Hacker

A hacker is an individual who intends to gain unauthorized access to a computer system.

B. ವರ್ಮ್

ಕಂಪ್ಯೂಟರ್ ವರ್ಮ್ ಎಂಬುದು ಒಂದು ರೀತಿಯ ಮಾಲ್ವೇರ್ ಆಗಿದ್ದು, ಸೋಂಕಿತ ವ್ಯವಸ್ಥೆಗಳಲ್ಲಿ ಸಕ್ರಿಯವಾಗಿರುವಾಗ ಇತರ ಕಂಪ್ಯೂಟರ್ಗಳನ್ನು ಸ್ವಯಂ-ನಕಲು ಮಾಡುವುದು ಮತ್ತು ಸೋಂಕಿಗೆ ಒಳಪಡಿಸುವುದು ಇದರ ಪ್ರಾಥಮಿಕ ಕಾರ್ಯವಾಗಿದೆ.

C. ರಾನ್ಸಮ್ವೇರ್

ರಾನ್ಸಮ್ವೇರ್ (ಸ್ಕೇರ್ವೇರ್) ಒಂದು ರೀತಿಯ ಮಾಲ್ವೇರ್ ಆಗಿದೆ (ಸಾಮಾನ್ಯವಾಗಿ ವರ್ಮ್) ಅದು ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ಫೈಲ್ಗಳನ್ನು ಪ್ರವೇಶಿಸದಂತೆ ಲಾಕ್ ಮಾಡುತ್ತದೆ.

D. ಟ್ರೋಜನ್ ಹಾರ್ಸ್

ಟ್ರೋಜನ್ ಹಾರ್ಸ್ ಸೌಮ್ಯವಾಗಿ ಕಾಣುತ್ತದೆ, ಆದರೆ ನಂತರ ನಿರೀಕ್ಷೆಗಿಂತ ಬೇರೆಯದನ್ನು ಮಾಡುತ್ತದೆ. ಸಾಮಾನ್ಯವಾಗಿ ವೈರಸ್ಗಳು ಅಥವಾ ಇತರ ದುರುದ್ದೇಶಪೂರಿತ ಕೋಡ್ ಅನ್ನು ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್ಗೆ ಪರಿಚಯಿಸುವ ಮಾರ್ಗವಾಗಿದೆ.

2. ಸಂಭಾವ್ಯ ಅನಗತ್ಯ ಪ್ರೋಗ್ರಾಂ (PUP): ಸಾಮಾನ್ಯವಾಗಿ ಬಳಕೆದಾರರ ತಿಳುವಳಿಕೆಯುಳ್ಳ ಒಪ್ಪಿಗೆಯಿಲ್ಲದೆಯೇ ಕಂಪ್ಯೂಟರ್ನಲ್ಲಿ ಸ್ವತಃ ಸ್ಥಾಪಿಸುವ ಪ್ರೋಗ್ರಾಂ.

A. ಆಯ್ಡ್ವೇರ್

ಬಳಕೆದಾರರು ನಿರ್ದಿಷ್ಟ ಸೈಟ್ಗಳಿಗೆ ಭೇಟಿ ನೀಡಿದಾಗ ಪ್ರದರ್ಶಿಸಲು ಪಾಪ್-ಅಪ್ ಜಾಹೀರಾತುಗಳಿಗೆ ಕರೆ ಮಾಡಲು ಆಯ್ಡ್ವೇರ್ ಅನ್ನು ಸಾಮಾನ್ಯವಾಗಿ ಬಳಸಲಾಗುತ್ತದೆ. ಕಿರಿಕಿರಿಯುಂಟುಮಾಡುವ ಸಂದರ್ಭದಲ್ಲಿ, ಆಡ್ವೇರ್ ಅನ್ನು ಸಾಮಾನ್ಯವಾಗಿ ಅಪರಾಧ ಚಟುವಟಿಕೆಗಳಿಗೆ ಬಳಸಲಾಗುವುದಿಲ್ಲ.

B. ಸ್ಪೈವೇರ್:

ಸ್ಪೈವೇರ್ ಬಳಕೆದಾರರ ಕೀಸ್ಟ್ರೋಕ್ಗಳು, ಇ-ಮೇಲ್, ತ್ವರಿತ ಸಂದೇಶಗಳು ಮತ್ತು ಮುಂತಾದ ಮಾಹಿತಿಯನ್ನು ಪಡೆಯಲು ಬಳಸುವ ಪ್ರೋಗ್ರಾಂ.

3. ಫಿಶಿಂಗ್:

ಹಣಕಾಸಿನ ಲಾಭಕ್ಕಾಗಿ ಗೌಪ್ಯ ಮಾಹಿತಿಯನ್ನು ಪಡೆಯಲು ಮೂರನೇ ವ್ಯಕ್ತಿಯಿಂದ ಯಾವುದೇ ಮೋಸಗೊಳಿಸುವ, ಆನ್ಲೈನ್ ಪ್ರಯತ್ನ.

4. ಹ್ಯಾಕರ್

ಹ್ಯಾಕರ್ ಎಂದರೆ ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್ಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶವನ್ನು ಪಡೆಯಲು ಉದ್ದೇಶಿಸಿರುವ ವ್ಯಕ್ತಿ.

5. CREDIT CARD FRAUD/THEFT

Theft of credit card data is one of the most feared occurrences on the Internet. Fear that credit card information will be stolen prevents users from making online purchases in many cases.

6. Spoofing

spoofing involves attempting to hide a true identity by using someone else's e-mail or IP address.

7. Spam (junk) Web sites also referred to as link farms; promise to offer products or services, but in fact are just collection of advertisement.

8. Denial of Service (DoS) attack: Hackers flood a Web site with useless pings or page requested that inundated the site's Web servers.

ENCRYPTION

Encryption is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the receiver.

The purpose of encryption is (a) to secure stored information and (b) to secure information transmission.

1. Message integrity- provides assurance that the message has not been altered.
2. Nonrepudiation—prevents the user from denying he or she sent the message.
3. Authentication—provides verification of the identity of the person (or computer) sending the message.
4. Confidentiality—gives assurance that the message was not read by others.

5. ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಂಚನೆ/ಕಳ್ಳತನ

ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಡೇಟಾದ ಕಳ್ಳತನವು ಇಂಟರ್ನೆಟ್‌ನಲ್ಲಿ ಹೆಚ್ಚು ಭಯಪಡುವ ಘಟನೆಗಳಲ್ಲಿ ಒಂದಾಗಿದೆ. ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಮಾಹಿತಿಯನ್ನು ಕದಿಯಲಾಗುತ್ತದೆ ಎಂಬ ಭಯವು ಅನೇಕ ಸಂದರ್ಭಗಳಲ್ಲಿ ಬಳಕೆದಾರರನ್ನು ಆನ್‌ಲೈನ್ ಖರೀದಿಗಳನ್ನು ಮಾಡುವುದನ್ನು ತಡೆಯುತ್ತದೆ.

6. ವಂಚನೆ: ವಂಚನೆಯು ಬೇರೊಬ್ಬರ ಇಮೇಲ್ ಅಥವಾ IP ವಿಳಾಸವನ್ನು ಬಳಸಿಕೊಂಡು ನಿಜವಾದ ಗುರುತನ್ನು ಮರೆಮಾಡಲು ಪ್ರಯತ್ನಿಸುವುದನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ.

7. ಸ್ಪ್ಯಾಮ್ (ಜಂಕ್) ವೆಬ್ ಸೈಟ್‌ಗಳನ್ನು ಲಿಂಕ್ ಫಾರ್ಮ್‌ಗಳು ಎಂದೂ ಕರೆಯಲಾಗುತ್ತದೆ; ಉತ್ಪನ್ನಗಳು ಅಥವಾ ಸೇವೆಗಳನ್ನು ನೀಡುವ ಭರವಸೆ, ಆದರೆ ವಾಸ್ತವವಾಗಿ ಕೇವಲ ಜಾಹೀರಾತಿನ ಸಂಗ್ರಹವಾಗಿದೆ.

8.ಸೇವೆ ನಿರಾಕರಣೆ (DoS) ದಾಳಿ: ಹ್ಯಾಕರ್‌ಗಳು ವೆಬ್‌ಸೈಟ್‌ಗೆ ಅನುಪಯುಕ್ತ ಪಿಂಗ್‌ಗಳು ಅಥವಾ ಪುಟವನ್ನು ವಿನಂತಿಸಿದರೆ ಅದು ಸೈಟ್‌ನ ವೆಬ್ ಸರ್ವರ್‌ಗಳನ್ನು ಮುಳುಗಿಸುತ್ತದೆ.

ಗೂಢಲಿಪೀಕರಣ

ಗೂಢಲಿಪೀಕರಣವು ಸರಳ ಪಠ್ಯ ಅಥವಾ ಡೇಟಾವನ್ನು ಸೈಫರ್ ಪಠ್ಯವಾಗಿ ಪರಿವರ್ತಿಸುವ ಪ್ರಕ್ರಿಯೆಯಾಗಿದ್ದು ಅದನ್ನು ಕಳುಹಿಸುವವರು ಮತ್ತು ಸ್ವೀಕರಿಸುವವರನ್ನು ಹೊರತುಪಡಿಸಿ ಬೇರೆಯವರು ಓದಲಾಗುವುದಿಲ್ಲ.

ಎನ್‌ಕ್ರಿಪ್ಶನ್‌ನ ಉದ್ದೇಶವು (ಎ) ಸಂಗ್ರಹಿಸಿದ ಮಾಹಿತಿಯನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸುವುದು ಮತ್ತು (ಬಿ) ಮಾಹಿತಿ ರವಾನೆಯನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸುವುದು.

1. ಸಂದೇಶ ಸಮಗ್ರತೆ- ಸಂದೇಶವನ್ನು ಬದಲಾಯಿಸಲಾಗಿಲ್ಲ ಎಂಬ ಭರವಸೆಯನ್ನು ನೀಡುತ್ತದೆ.
2. ನಿರಾಕರಣೆ-ಬಳಕೆದಾರನು ಅವನು ಅಥವಾ ಅವಳು ಕಳುಹಿಸಿದ ಸಂದೇಶವನ್ನು ನಿರಾಕರಿಸುವುದನ್ನು ತಡೆಯುತ್ತದೆ.
3. ದೃಢೀಕರಣ-ಸಂದೇಶವನ್ನು ಕಳುಹಿಸುವ ವ್ಯಕ್ತಿಯ (ಅಥವಾ ಕಂಪ್ಯೂಟರ್) ಗುರುತಿನ ಪರಿಶೀಲನೆಯನ್ನು ಒದಗಿಸುತ್ತದೆ.
4. ಗೌಪ್ಯತೆ-ಸಂದೇಶವನ್ನು ಇತರರು ಓದಿಲ್ಲ ಎಂಬ ಭರವಸೆಯನ್ನು ನೀಡುತ್ತದೆ.

This transformation of plain text to cipher text is accomplished by using a key or cipher. A key (or cipher) is any method for transforming plain text to cipher text.

Substitution cipher: every occurrence of a given letters is replaced systematically by another letter.

Transposition cipher: the ordering of the letters in each word is changed in some systematic way.

Symmetric Key Cryptography

In order to decipher these messages, the receiver would have to know the secret cipher that was used to encrypt the plain text. This is called symmetric key cryptography or secret key cryptography.

In symmetric key cryptography, both the sender and the receiver use the same key to encrypt and decrypt the message.

PUBLIC KEY CRYPTOGRAPHY

Steps:

1. The sender creates a digital message.
2. The sender obtains the recipient's public key from a public directory and applies it to the message.
3. Application of the recipient's key produces an encrypted cipher text message.
4. The encrypted message is sent over the Internet.

5. The recipient uses his/her private key to decrypt the message.

ಸರಳ ಪಠ್ಯದಿಂದ ಸೈಫರ್ ಪಠ್ಯಕ್ಕೆ ಈ ರೂಪಾಂತರವನ್ನು ಕೀ ಅಥವಾ ಸೈಫರ್ ಬಳಸಿ ಸಾಧಿಸಲಾಗುತ್ತದೆ. ಒಂದು ಕೀ (ಅಥವಾ ಸೈಫರ್) ಸರಳ ಪಠ್ಯವನ್ನು ಸೈಫರ್ ಪಠ್ಯಕ್ಕೆ ಪರಿವರ್ತಿಸುವ ಯಾವುದೇ ವಿಧಾನವಾಗಿದೆ.

ಪರ್ಯಾಯ ಸೈಫರ್: ಸರಳ ಪಠ್ಯದಿಂದ ಸೈಫರ್ ಪಠ್ಯಕ್ಕೆ ಈ ರೂಪಾಂತರವನ್ನು ಕೀ ಅಥವಾ ಸೈಫರ್ ಬಳಸಿ ಸಾಧಿಸಲಾಗುತ್ತದೆ. ಒಂದು ಕೀ (ಅಥವಾ ಸೈಫರ್) ಸರಳ ಪಠ್ಯವನ್ನು ಸೈಫರ್ ಪಠ್ಯಕ್ಕೆ ಪರಿವರ್ತಿಸುವ ಯಾವುದೇ ವಿಧಾನವಾಗಿದೆ.

ವರ್ಗಾವಣೆ ಸೈಫರ್: ಪ್ರತಿ ಪದದಲ್ಲಿನ ಅಕ್ಷರಗಳ ಕ್ರಮವನ್ನು ಕೆಲವು ವ್ಯವಸ್ಥಿತ ರೀತಿಯಲ್ಲಿ ಬದಲಾಯಿಸಲಾಗುತ್ತದೆ.

ಸಿಮೆಟ್ರಿಕ್ ಕೀ ಕ್ರಿಪ್ಟೋಗ್ರಫಿ

ಈ ಸಂದೇಶಗಳನ್ನು ಅರ್ಥಮಾಡಿಕೊಳ್ಳಲು, ರಿಸೀವರ್ ಸರಳ ಪಠ್ಯವನ್ನು ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಲು ಬಳಸಿದ ರಹಸ್ಯ ಸೈಫರ್ ಅನ್ನು ತಿಳಿದುಕೊಳ್ಳಬೇಕು. ಇದನ್ನು ಸಿಮೆಟ್ರಿಕ್ ಕೀ ಕ್ರಿಪ್ಟೋಗ್ರಫಿ ಅಥವಾ ಸೀಕ್ರೆಟ್ ಕೀ ಕ್ರಿಪ್ಟೋಗ್ರಫಿ ಎಂದು ಕರೆಯಲಾಗುತ್ತದೆ.

ಸಮ್ಮಿತೀಯ ಕೀ ಕ್ರಿಪ್ಟೋಗ್ರಫಿಯಲ್ಲಿ, ಕಳುಹಿಸುವವರು ಮತ್ತು ಸ್ವೀಕರಿಸುವವರು ಸಂದೇಶವನ್ನು ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಲು ಮತ್ತು ಡೀಕ್ರಿಪ್ಟ್ ಮಾಡಲು ಒಂದೇ ಕೀಲಿಯನ್ನು ಬಳಸುತ್ತಾರೆ.

ಸಾರ್ವಜನಿಕ ಕೀ ಕ್ರಿಪ್ಟೋಗ್ರಫಿ

ಹಂತಗಳು:

1. ಕಳುಹಿಸುವವರು ಡಿಜಿಟಲ್ ಸಂದೇಶವನ್ನು ರಚಿಸುತ್ತಾರೆ.
2. ಕಳುಹಿಸುವವರು ಸಾರ್ವಜನಿಕ ಡೈರೆಕ್ಟರಿಯಿಂದ ಸ್ವೀಕರಿಸುವವರ ಸಾರ್ವಜನಿಕ ಕೀಲಿಯನ್ನು ಪಡೆದುಕೊಳ್ಳುತ್ತಾರೆ ಮತ್ತು ಅದನ್ನು ಸಂದೇಶಕ್ಕೆ ಅನ್ವಯಿಸುತ್ತಾರೆ.
3. ಸ್ವೀಕರಿಸುವವರ ಕೀಲಿಯ ಅಪ್ಲಿಕೇಶನ್ ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಿದ ಸೈಫರ್ ಪಠ್ಯ ಸಂದೇಶವನ್ನು ಉತ್ಪಾದಿಸುತ್ತದೆ.
4. ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಿದ ಸಂದೇಶವನ್ನು ಇಂಟರ್ನೆಟ್ ಮೂಲಕ ಕಳುಹಿಸಲಾಗುತ್ತದೆ.
5. ಸಂದೇಶವನ್ನು ಡೀಕ್ರಿಪ್ಟ್ ಮಾಡಲು ಸ್ವೀಕರಿಸುವವರು ಅವನ/ಅವಳ ಖಾಸಗಿ ಕೀಲಿಯನ್ನು ಬಳಸುತ್ತಾರೆ.

Tools available to achieve website security

1. Encryption
2. Network security protocols
3. Virtual private networks
4. Firewalls
5. Proxy servers
6. Intrusion detection/prevention
7. Automated software updates
8. Antivirus software
9. Access controls
10. Authentication procedures

HOW AN ONLINE CREDIT CARD TRANSACTION WORKS

Because credit and debit cards are the dominant form of online payment, it is important to understand how they work and to recognize the strengths and weaknesses of this payment system.

There are five parties involved in an online credit card purchase: consumer, merchant, clearing house, merchant bank (sometimes called the “acquiring bank”), and the consumer’s card issuing bank.

An online credit card transaction begins with a purchase (1) When a consumer wants to make a purchase, he or she adds the item to the merchant’s shopping cart. When the consumer wants to pay for the items in the shopping cart, a secure tunnel through the Internet is created using SSL/TLS. Using encryption, SSL/TLS secures the session during which credit card information will be sent to the merchant and protects the information from interlopers on the Internet (2). SSL does not authenticate either the merchant or the consumer. The transacting parties must trust one another.

ವೆಬ್‌ಸೈಟ್ ಸುರಕ್ಷತೆಯನ್ನು ಸಾಧಿಸಲು ಲಭ್ಯವಿರುವ ಸಾಧನಗಳು

1. ಗೂಢಲಿಪೀಕರಣ
2. ನೆಟ್ವರ್ಕ್ ಭದ್ರತಾ ಶಿಷ್ಟಾಚಾರಗಳು

3. ವರ್ಚುವಲ್ ಖಾಸಗಿ ಜಾಲಗಳು
4. ಫೈರ್‌ವಾಲ್‌ಗಳು
5. ಪ್ರಾಕ್ಸಿ ಸರ್ವರ್‌ಗಳು
6. ಒಳನುಗ್ಗುವಿಕೆ ಪತ್ತೆ/ತಡೆಗಟ್ಟುವಿಕೆ
7. ಸ್ವಯಂಚಾಲಿತ ಸಾಫ್ಟ್‌ವೇರ್ ನವೀಕರಣಗಳು
8. ಆಂಟಿವೈರಸ್ ಸಾಫ್ಟ್‌ವೇರ್‌ಗಳು
9. ಪ್ರವೇಶ ನಿಯಂತ್ರಣಗಳು
10. ದೃಢೀಕರಣ ಕಾರ್ಯವಿಧಾನಗಳು

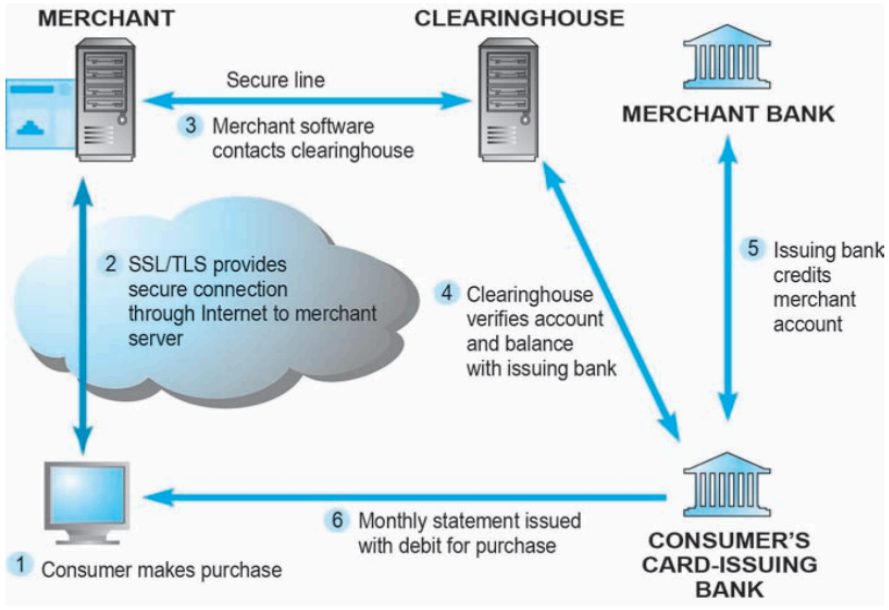
ಆನ್‌ಲೈನ್ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಹಿವಾಟು ಹೇಗೆ ಕೆಲಸ ಮಾಡುತ್ತದೆ

ಕ್ರೆಡಿಟ್ ಮತ್ತು ಡೆಬಿಟ್ ಕಾರ್ಡ್‌ಗಳು ಆನ್‌ಲೈನ್ ಪಾವತಿಯ ಪ್ರಮುಖ ರೂಪವಾಗಿರುವುದರಿಂದ, ಅವು ಹೇಗೆ ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತವೆ ಎಂಬುದನ್ನು ಅರ್ಥಮಾಡಿಕೊಳ್ಳುವುದು ಮತ್ತು ಈ ಪಾವತಿ ವ್ಯವಸ್ಥೆಯ ಸಾಮರ್ಥ್ಯ ಮತ್ತು ದೌರ್ಬಲ್ಯಗಳನ್ನು ಗುರುತಿಸುವುದು ಮುಖ್ಯವಾಗಿದೆ.

ಆನ್‌ಲೈನ್ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಖರೀದಿಯಲ್ಲಿ ಐದು ಪಕ್ಷಗಳು ಭಾಗಿಯಾಗಿವೆ: ಗ್ರಾಹಕ, ವ್ಯಾಪಾರಿ, ಕ್ಲಿಯರಿಂಗ್ ಹೌಸ್, ಮರ್ಚೆಂಟ್ ಬ್ಯಾಂಕ್ (ಕೆಲವೊಮ್ಮೆ "ಸ್ವಾಧೀನಪಡಿಸಿಕೊಳ್ಳುವ ಬ್ಯಾಂಕ್" ಎಂದು ಕರೆಯಲಾಗುತ್ತದೆ), ಮತ್ತು ಗ್ರಾಹಕರ ಕಾರ್ಡ್ ನೀಡುವ ಬ್ಯಾಂಕ್.

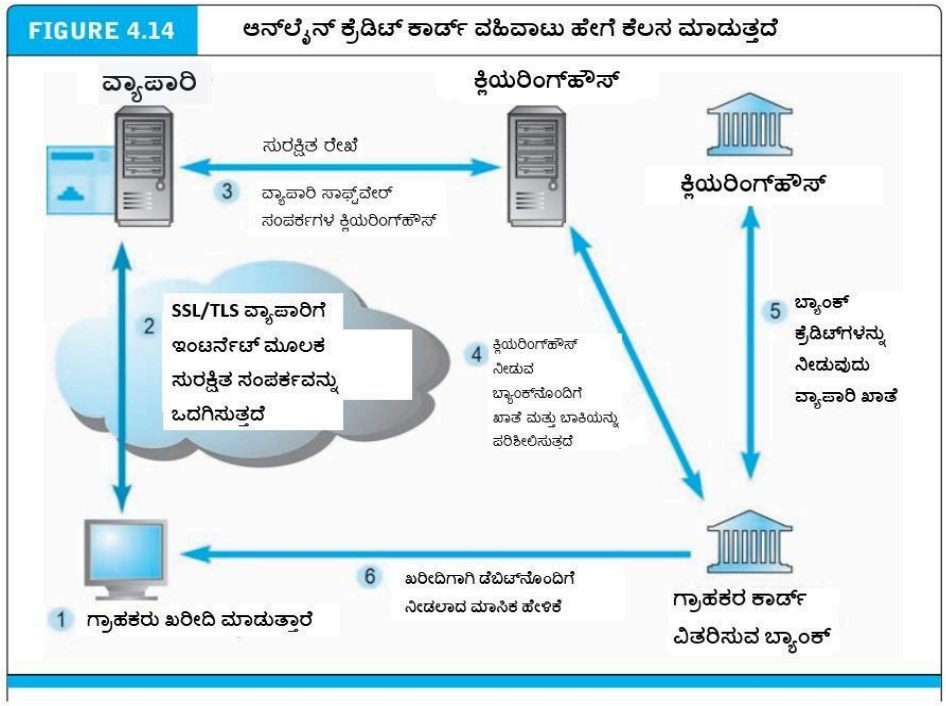
ಆನ್‌ಲೈನ್ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಹಿವಾಟು ಖರೀದಿಯೊಂದಿಗೆ ಪ್ರಾರಂಭವಾಗುತ್ತದೆ (1) ಗ್ರಾಹಕರು ಖರೀದಿಯನ್ನು ಮಾಡಲು ಬಯಸಿದಾಗ, ಅವನು ಅಥವಾ ಅವಳು ಐಟಂ ಅನ್ನು ವ್ಯಾಪಾರಿಯ ಶಾಪಿಂಗ್ ಕಾರ್ಟ್‌ಗೆ ಸೇರಿಸುತ್ತಾರೆ. ಗ್ರಾಹಕರು ಶಾಪಿಂಗ್ ಕಾರ್ಟ್‌ನಲ್ಲಿರುವ ವಸ್ತುಗಳನ್ನು ಪಾವತಿಸಲು ಬಯಸಿದಾಗ, ಇಂಟರ್ನೆಟ್ ಮೂಲಕ ಸುರಕ್ಷಿತ ಸುರಂಗವನ್ನು SSL/TLS ಬಳಸಿ ರಚಿಸಲಾಗುತ್ತದೆ. ಗೂಢಲಿಪೀಕರಣವನ್ನು ಬಳಸಿಕೊಂಡು, SSL/TLS ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಮಾಹಿತಿಯನ್ನು ವ್ಯಾಪಾರಿಗೆ ಕಳುಹಿಸುವ ಅಧಿವೇಶನವನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸುತ್ತದೆ ಮತ್ತು ಇಂಟರ್ನೆಟ್‌ನಲ್ಲಿನ ಮಧ್ಯಸ್ಥಿಕೆದಾರರಿಂದ ಮಾಹಿತಿಯನ್ನು ರಕ್ಷಿಸುತ್ತದೆ (2). SSL ವ್ಯಾಪಾರಿ ಅಥವಾ ಗ್ರಾಹಕರನ್ನು ದೃಢೀಕರಿಸುವುದಿಲ್ಲ. ವಹಿವಾಟು ನಡೆಸುವ ಪಕ್ಷಗಳು ಒಬ್ಬರನ್ನೊಬ್ಬರು ನಂಬಬೇಕು.

FIGURE 4.14 HOW AN ONLINE CREDIT CARD TRANSACTION WORKS



Once the consumer credit card information is received by the merchant, the merchant software contacts a clearinghouse (3). As previously noted, a clearinghouse is a financial intermediary that authenticates credit cards and verifies account balances. The clearinghouse contacts the issuing bank to verify the account information (4). Once verified, the issuing bank credits the account of the merchant at the merchant's bank (usually this occurs at night in a batch process) (5). The debit to the consumer account is transmitted to the consumer in a monthly statement (6).

ಗ್ರಾಹಕರ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಮಾಹಿತಿಯನ್ನು ವ್ಯಾಪಾರಿ ಸ್ವೀಕರಿಸಿದ ನಂತರ, ವ್ಯಾಪಾರಿ ಸಾಫ್ಟ್‌ವೇರ್ ಕ್ಲಿಯರಿಂಗ್‌ಹೌಸ್ ಅನ್ನು ಸಂಪರ್ಕಿಸುತ್ತದೆ (3). ಹಿಂದೆ ಗಮನಿಸಿದಂತೆ, ಕ್ಲಿಯರಿಂಗ್‌ಹೌಸ್ ಎನ್ನುವುದು ಹಣಕಾಸಿನ ಮಧ್ಯವರ್ತಿಯಾಗಿದ್ದು ಅದು ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್‌ಗಳನ್ನು ದೃಢೀಕರಿಸುತ್ತದೆ ಮತ್ತು ಖಾತೆಯ ಬಾಕಿಗಳನ್ನು ಪರಿಶೀಲಿಸುತ್ತದೆ. ಖಾತೆಯ ಮಾಹಿತಿಯನ್ನು ಪರಿಶೀಲಿಸಲು ಕ್ಲಿಯರಿಂಗ್‌ಹೌಸ್ ನೀಡುವ ಬ್ಯಾಂಕ್ ಅನ್ನು ಸಂಪರ್ಕಿಸುತ್ತದೆ (4). ಒಮ್ಮೆ ಪರಿಶೀಲಿಸಿದ ನಂತರ, ವಿತರಿಸುವ ಬ್ಯಾಂಕ್ ವ್ಯಾಪಾರಿಯ ಬ್ಯಾಂಕ್‌ನಲ್ಲಿ ವ್ಯಾಪಾರಿಯ ಖಾತೆಯನ್ನು ಕ್ರೆಡಿಟ್ ಮಾಡುತ್ತದೆ (ಸಾಮಾನ್ಯವಾಗಿ ಇದು ಬ್ಯಾಚ್ ಪ್ರಕ್ರಿಯೆಯಲ್ಲಿ ರಾತ್ರಿಯಲ್ಲಿ ಸಂಭವಿಸುತ್ತದೆ) (5). ಗ್ರಾಹಕರ ಖಾತೆಗೆ ಡೆಬಿಟ್ ಮಾಸಿಕ ಹೇಳಿಕೆಯಲ್ಲಿ ಗ್ರಾಹಕರಿಗೆ ರವಾನೆಯಾಗುತ್ತದೆ (6).



E-PAYMENT (Electronic Payment)

An e-payment or Electronic Payment system allows customers to pay for the services via electronic methods. They are also known as online payment systems. Normally e-payment is done via debit, credit cards, direct bank deposits, and e-checks, other alternative e-payment methods like e-wallets, bitcoin, cryptocurrencies, bank transfers are also gaining popularity.

Types of e-payment system

1. **Internet banking** – In this case, the payment is done by digitally transferring the funds over the internet from one bank account to another.

Some popular modes of net banking are NEFT, RTGS, IMPS.

2. **Card payments** – Card payments are done via cards e.g. credit cards, debit cards, smart cards, stored valued cards, etc. An electronic payment accepting device initiates the online payment transfer via card.

   Credit/ Debit card – An e-payment method where the card is required for making payments through an electronic device.

3. **E-wallet** – Very popular among customers, an E-wallet is a form of prepaid account, where customer's account information like credit/ debit card information is stored allowing quick, seamless, and smooth flow of the transaction.

4. **QR payments** – QR code-enabled payments have become immensely popular. QR code stands for 'Quick Response' code, a code that contains a pixel pattern of barcodes or squares arranged in a square grid. Each part of the code contains information. This information can be merchant's details, transaction details, etc. To make payments, one must scan the QR code with a mobile device.

ಇ-ಪಾವತಿ (ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಪಾವತಿ)

ಇ-ಪಾವತಿ ಅಥವಾ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಪಾವತಿ ವ್ಯವಸ್ಥೆಯು ಗ್ರಾಹಕರಿಗೆ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ವಿಧಾನಗಳ ಮೂಲಕ ಸೇವೆಗಳಿಗೆ ಪಾವತಿಸಲು ಅನುವು ಮಾಡಿಕೊಡುತ್ತದೆ. ಅವುಗಳನ್ನು ಆನ್ ಲೈನ್ ಪಾವತಿ ವ್ಯವಸ್ಥೆಗಳು ಎಂದೂ ಕರೆಯಲಾಗುತ್ತದೆ. ಸಾಮಾನ್ಯವಾಗಿ ಇ-ಪಾವತಿಯನ್ನು ಡೆಬಿಟ್, ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್‌ಗಳು, ನೇರ ಬ್ಯಾಂಕ್ ಠೇವಣಿಗಳು ಮತ್ತು ಇ-ಚೆಕ್‌ಗಳ ಮೂಲಕ ಮಾಡಲಾಗುತ್ತದೆ, ಇ-ವ್ಯಾಲೆಟ್‌ಗಳು, ಬಿಟ್‌ಕಾಯಿನ್, ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿಗಳು, ಬ್ಯಾಂಕ್ ವರ್ಗಾವಣೆಗಳಂತಹ ಇತರ ಪರ್ಯಾಯ ಇ-ಪಾವತಿ ವಿಧಾನಗಳು ಸಹ ಜನಪ್ರಿಯತೆಯನ್ನು ಪಡೆಯುತ್ತಿವೆ.

ಇ-ಪಾವತಿ ವ್ಯವಸ್ಥೆಯ ವಿಧಗಳು

1. **ಇಂಟರ್ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ -** ಈ ಸಂದರ್ಭದಲ್ಲಿ, ಒಂದು ಬ್ಯಾಂಕ್ ಖಾತೆಯಿಂದ ಇನ್ನೊಂದಕ್ಕೆ ಇಂಟರ್ನೆಟ್ ಮೂಲಕ ಹಣವನ್ನು ಡಿಜಿಟಲ್ ಆಗಿ ವರ್ಗಾಯಿಸುವ ಮೂಲಕ ಪಾವತಿ ಮಾಡಲಾಗುತ್ತದೆ. ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ನ ಕೆಲವು ಜನಪ್ರಿಯ ವಿಧಾನಗಳೆಂದರೆ, **ನೆಫ್ಟ್, ಆರ್ ಟಿಜಿಎಸ್, ಐಎಂಪಿಎಸ್.**

2. **ಕಾರ್ಡ್ ಪಾವತಿಗಳು -** ಕಾರ್ಡ್ ಪಾವತಿಗಳನ್ನು ಕಾರ್ಡ್‌ಗಳ ಮೂಲಕ ಮಾಡಲಾಗುತ್ತದೆ ಉದಾ. ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್‌ಗಳು, ಡೆಬಿಟ್ ಕಾರ್ಡ್‌ಗಳು, ಸ್ಮಾರ್ಟ್ ಕಾರ್ಡ್‌ಗಳು, ಸಂಗ್ರಹಿಸಿದ ಮೌಲ್ಯದ ಕಾರ್ಡ್‌ಗಳು, ಇತ್ಯಾದಿ. ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಪಾವತಿ ಸ್ವೀಕರಿಸುವ ಸಾಧನವು ಕಾರ್ಡ್ ಮೂಲಕ ಆನ್‌ಲೈನ್ ಪಾವತಿ ವರ್ಗಾವಣೆಯನ್ನು ಪ್ರಾರಂಭಿಸುತ್ತದೆ.
   ಕ್ರೆಡಿಟ್/ಡೆಬಿಟ್ ಕಾರ್ಡ್: ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಸಾಧನದ ಮೂಲಕ ಪಾವತಿಗಳನ್ನು ಮಾಡಲು ಕಾರ್ಡ್ ಅಗತ್ಯವಿರುವ ಇ-ಪಾವತಿ ವಿಧಾನ.
3. **ಇ-ವ್ಯಾಲೆಟ್** - ಗ್ರಾಹಕರಲ್ಲಿ ಬಹಳ ಜನಪ್ರಿಯವಾಗಿದೆ, ಇ-ವ್ಯಾಲೆಟ್ ಪ್ರಿಪೇಯ್ಡ್ ಖಾತೆಯ ಒಂದು ರೂಪವಾಗಿದೆ, ಅಲ್ಲಿ ಕ್ರೆಡಿಟ್/ಡೆಬಿಟ್ ಕಾರ್ಡ್ ಮಾಹಿತಿಯಂತಹ ಗ್ರಾಹಕರ ಖಾತೆಯ ಮಾಹಿತಿಯನ್ನು ಸಂಗ್ರಹಿಸಲಾಗುತ್ತದೆ ಮತ್ತು ವಹಿವಾಟಿನ ತ್ವರಿತ, ತಡೆರಹಿತ ಮತ್ತು ಸುಗಮ ಹರಿವನ್ನು ಅನುಮತಿಸುತ್ತದೆ.

4. **QR ಪಾವತಿಗಳು** - QR ಕೋಡ್-ಸಕ್ರಿಯಗೊಳಿಸಿದ ಪಾವತಿಗಳು ಅಗಾಧವಾಗಿ ಜನಪ್ರಿಯವಾಗಿವೆ. QR ಕೋಡ್ ಎಂದರೆ 'ಕ್ವಿಕ್ ರೆಸ್ಪಾನ್ಸ್' ಕೋಡ್, ಬಾರ್‌ಕೋಡ್‌ಗಳ ಪಿಕ್ಸೆಲ್ ಮಾದರಿಯನ್ನು ಹೊಂದಿರುವ ಕೋಡ್ ಅಥವಾ ಚೌಕ ಗ್ರಿಡ್‌ನಲ್ಲಿ ಜೋಡಿಸಲಾದ ಚೌಕಗಳು. ಕೋಡ್‌ನ ಪ್ರತಿಯೊಂದು ಭಾಗವು ಮಾಹಿತಿಯನ್ನು ಒಳಗೊಂಡಿದೆ. ಈ ಮಾಹಿತಿಯು ವ್ಯಾಪಾರಿಯ ವಿವರಗಳು, ವಹಿವಾಟಿನ ವಿವರಗಳು ಇತ್ಯಾದಿಯಾಗಿರಬಹುದು. ಪಾವತಿಗಳನ್ನು ಮಾಡಲು, ಒಬ್ಬರು ಮೊಬೈಲ್ ಸಾಧನದೊಂದಿಗೆ QR ಕೋಡ್ ಅನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಬೇಕು.

5. **UPI payments** – NPCI (National Payment Corporation of India) has developed an instant real-time payment system to facilitate interbank transactions.
   This payment system is titled UPI(Unified Payment Interface). Payments via UPI can be made via an app on a mobile device.

   Examples: BHIM, PAYTM, PHONEPE, GPAY.

Important questions

1-Mark

1. What is E-Commerce security?
2. What is E-Payment?
3. Write any two Antivirus software's.
4. What is Encryption?
5. What is malware?

5-Marks

1. What is encryption? Explain.
2. What are the tools available to achieve website security.
3. How an online credit cart transaction works? Explain.

10-Marks

1. What is E-Payment? Explain the types.
2. What is security threat? Explain different types of security threats.

5. **ಯುಪಿಐ ಪಾವತಿಗಳು** - ಎನ್‌ಪಿಸಿಐ (ನ್ಯಾಷನಲ್ ಪೇಮೆಂಟ್ ಕಾರ್ಪೊರೇಷನ್ ಆಫ್ ಇಂಡಿಯಾ) ಅಂತರ ಬ್ಯಾಂಕ್ ವಹಿವಾಟುಗಳನ್ನು ಸುಲಭಗೊಳಿಸಲು ತ್ವರಿತ ನೈಜ-ಸಮಯದ ಪಾವತಿ ವ್ಯವಸ್ಥೆಯನ್ನು ಅಭಿವೃದ್ಧಿಪಡಿಸಿದೆ.
   ಈ ಪಾವತಿ ವ್ಯವಸ್ಥೆಯನ್ನು ಯುಪಿಐ (ಏಕೀಕೃತ ಪಾವತಿ ಇಂಟರ್ಫೇಸ್) ಎಂದು ಹೆಸರಿಸಲಾಗಿದೆ.
   ಯುಪಿಐ ಮೂಲಕ ಪಾವತಿಗಳನ್ನು ಮೊಬೈಲ್ ಸಾಧನದಲ್ಲಿ ಅಪ್ಲಿಕೇಶನ್ ಮೂಲಕ ಮಾಡಬಹುದು.

   ಉದಾಹರಣೆಗಳು: BHIM, PAYTM, PHONEPE, GPAY.

ಪ್ರಮುಖ ಪ್ರಶ್ನೆಗಳು

1 - ಅಂಕ

1. ಇ-ಕಾಮರ್ಸ್ ಭದ್ರತೆ ಎಂದರೇನು?
2. ಇ-ಪಾವತಿ ಎಂದರೇನು?
3. ಯಾವುದಾದರೂ ಎರಡು ಆಂಟಿವೈರಸ್ ಸಾಫ್ಟ್‌ವೇರ್‌ಗಳನ್ನು ಬರೆಯಿರಿ.
4. ಎನ್‌ಕ್ರಿಪ್ಶನ್(ಗೂಢಲಿಪೀಕರಣ) ಎಂದರೇನು?
5. ಮಾಲ್ವೇರ್ ಎಂದರೇನು?

5-ಅಂಕಗಳು

1. ಎನ್‌ಕ್ರಿಪ್ಶನ್(ಗೂಢಲಿಪೀಕರಣ) ಎಂದರೇನು? ವಿವರಿಸಿ.
2. ವೆಬ್‌ಸೈಟ್ ಸುರಕ್ಷತೆಯನ್ನು ಸಾಧಿಸಲು ಲಭ್ಯವಿರುವ ಸಾಧನಗಳು ಯಾವುವು.
3. ಆನ್‌ಲೈನ್ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಹಿವಾಟು ಹೇಗೆ ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತದೆ? ವಿವರಿಸಿ.

10-ಅಂಕಗಳು

1. ಇ-ಪಾವತಿ ಎಂದರೇನು? ವಿಧಗಳನ್ನು ವಿವರಿಸಿ.
2. ಭದ್ರತಾ ಬೆದರಿಕೆ ಎಂದರೇನು? ವಿವಿಧ ರೀತಿಯ ಭದ್ರತಾ ಬೆದರಿಕೆಗಳನ್ನು ವಿವರಿಸಿ.