Mobile commerce, also known as m-commerce or mcommerce, is the use of wireless handheld devices like cellphones and tablets to conduct commercial transactions online, including the purchase and sale of products, [online banking](https://www.investopedia.com/terms/o/onlinebanking.asp), and paying bills. The use of m-commerce activity is on the rise. According to market research company Statista, mobile commerce sales in the United States were an estimated $207.2 billion in 2017.

### **KEY TAKEAWAYS**

* Mobile commerce refers to business or purchases conducted over mobile devices like cellphones or tablets.
* Mobile commerce has increased rapidly as security issues have been resolved.
* Companies like Apple and Google have introduced their own mobile commerce services.

Applications of mobile Commerse:

****1. Traffic:****

During travelling in traffic if we require to know road situation,latest news and when if feel more stress in driving then can play music and other important broadcast data are received through digital audio broadcasting(DAB).If we forget the road then we can know our exact location with the help of [global positioning system](https://en.wikipedia.org/wiki/Global_Positioning_System" \t "https://medium.com/@rmsrn.85/_blank) (GPS).In case if got accident then can to inform police and ambulance via an emergency call to service provider, which help to improve organization and save time & money.

****2. Emergencies Situation:****

To play vital role in medical sector can hire an ambulance with great quality wireless connection and help of this can carry significant information about injured persons. The useful step can prepare for particular accident and doctor can consulted for diagnosis. Only Wireless networks work of communication in nature disaster2 such as earthquakes, tsunami,flood and fire .In worst conditions only decentralized, wireless ad-hoc networks survive.Means that can handle Emergencies situation by mobile computing easily.

****3. Use in Business:****

As per business point of view CEO help of this computing system can represent the presentation at the front of their clients while can access hot news of

market.Help of video conference could be discuss at the topic without hindrance any time.Other side if travelling salesman want to access company database as

per requirement then can be retrieved data on his wireless device and maintain the consistency company’s database. Cause of these every employee are

updated up to date.

****4. Credit Card Verification:****

Credit card verification using this computing most secure.In respect of Sale terminals(POS) when customer buy items in malls and other small shops when

and pay bill in form of swap credit card for transactions then need to establish network in between POS terminal and bank central computer then over

protected cellular network verify the credential information of card fastly, if match it then proceed further otherwise denied get boost up speed of

transaction process and relieve the burden at the POS network.

****5. Replacement of Fixed Networks:****

Wired network has been replaced in wireless network e.g. trade shows, remote sensors and historical buildings. in wired networks ,weather forecasting,

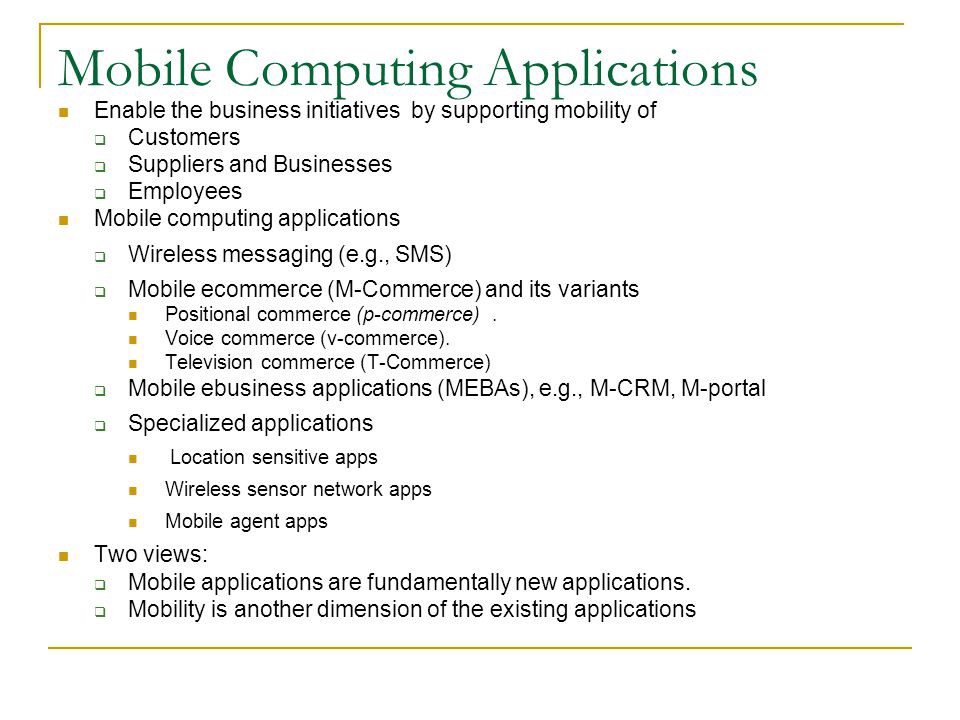
earthquake detection and to get environmental data are impossible .This is possible only in adapting replacement of fixed networks in this computing.

****6. Infotainment:****

Wireless networks are capable to deliver latest information at any suitable regions and can download knowledge about concert at morning through wireless

network that concert is conducting in any region as well as Another growing field of wireless network applications lies in entertainment and games to

enable, e.g., ad-hoc gaming networks as soon as people meet to play together.So Infotainment by wireless computing is more easy.

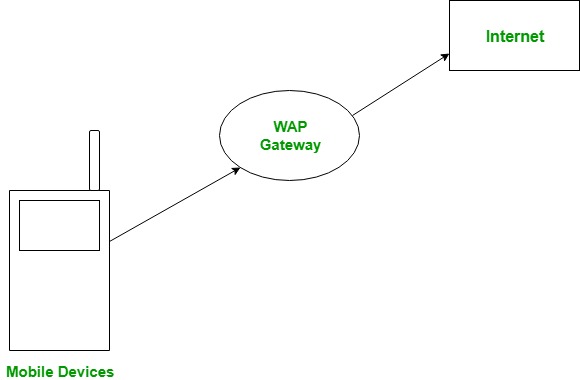


WAP:-

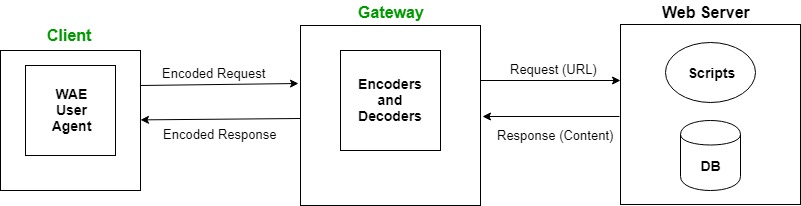
# Wireless Application Protocol

**WAP** stands for **Wireless Application Protocol**. It is a protocol designed for micro-browsers and it enables the access of internet in the mobile devices. It uses the mark-up language WML (Wireless Markup Language and not HTML), WML is defined as XML 1.0 application. It enables creating web applications for mobile devices. In 1998, *WAP Forum* was founded by Ericson, Motorola, Nokia and Unwired Planet whose aim was to standardize the various wireless technologies via protocols.

WAP protocol was resulted by the joint efforts of the various members of WAP Forum. In 2002, WAP forum was merged with various other forums of the industry resulting in the formation of **Open Mobile Alliance (OMA)**.

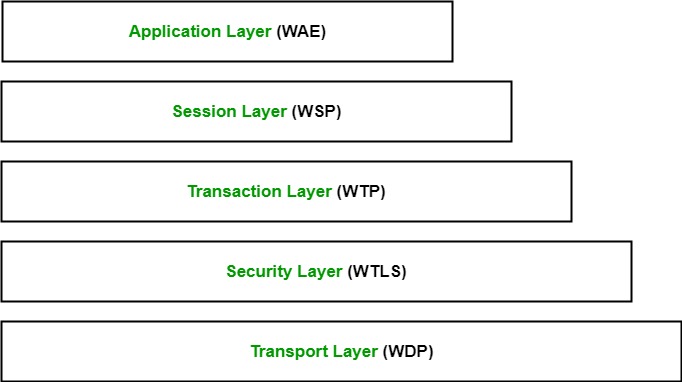


**WAP Model:**  
The user opens the mini-browser in a mobile device. He selects a website that he wants to view. The mobile device sends the URL encoded request via network to a WAP gateway using WAP protocol.



The WAP gateway translates this WAP request into a conventional HTTP URL request and sends it over the internet. The request reaches to a specified Web server and it processes the request just as it would have processed any other request and sends the response back to the mobile device through WAP gateway in WML file which can be seen in the micro-browser.

**WAP Protocol stack:**



1. **Application Layer:**  
   This layer contains the *Wireless Application Environment (WAE)*. It contains mobile device specifications and content development programming languages like WML.
2. **Session Layer:**  
   This layer contains *Wireless Session Protocol (WSP)*. It provides fast connection suspension and reconnection.
3. **Transaction Layer:**  
   This layer contains *Wireless Transaction Protocol (WTP)*. It runs on top of UDP (User Datagram Protocol) and is a part of TCP/IP and offers transaction support.
4. **Security Layer:**  
   This layer contains *Wireless Transaction Layer Security (WTLS)*. It offers data integrity, privacy and authentication.
5. **Transport Layer:**  
   This layer contains *Wireless Datagram Protocol*. It presents consistent data format to higher layers of WAP protocol stack.

## **Definition - What does *Mobile Information Device Profile (MIDP)* mean?**

Mobile Information Device Profile (MIDP) is a specification for the use of Java technology for mobile devices. In the context of software development, MIDP sits on top of the Connected Limited Device Configuration (CLDC).  
  
Because MIDP is primarily used with CLDC, which is designed for highly constrained devices with limited CPUs, screen size, RAM, battery power and user interface, midlets are ideal for low-end cell phones.  
  
Applications written with MIDP are normally designed for cell phones and PDAs. They are known as midlets.

# Types of firewall and possible attacks

No one can deny the fact that the dynamic rise of the Internet has brought the world closer. But at the same time, it has left us with different kinds of security threats. To ensure the confidentiality and integrity of valuable information of a corporate network from the outside attacks, we must have some robust mechanism. This is where the **Firewall** comes into picture.

It can be compared with a security guard standing at the entrance of a minister’s home. He keeps an eye on everyone and physically checks every person who wishes to enter the house. It won’t allow a person to enter if he/she is carrying a harmful object like a knife, gun etc. Similarly, even if the person doesn’t possess any banned object but appears suspicious, the guard can still prevent that person’s entry.

The firewall acts as a guard. It guards a corporate network acting as a shield between the inside network and the outside world. All the traffic in either direction must pass through the firewall. It then decides whether the traffic is allowed to flow or not. The firewall can be implemented as hardware and software, or a combination of both.

IMG_256

**Types of Firewalls:**

1. **Packet Filters –**  
   It works in the **network layer** of the OSI Model. It applies a set of rules (based on the contents of IP and transport header fields) on each packet and based on the outcome, decides to either forward or discard the packet.

For example, a rule could specify to block all incoming traffic from a certain IP address or disallow all traffic that uses UDP protocol. If there is no match with any predefined rules, it will take default action. The default action can be to ‘discard all packets’ or to ‘accept all packets’.

**Security threats** to Packet Filters:

* 1. **IP address Spoofing:**  
     In this kind of attack, an intruder from the outside tries to send a packet towards the internal corporate network with the source IP address set equal to one of the IP address of internal users.  
     **Prevention:**  
     Firewall can defeat this attack if it discards all the packets that arrive at the incoming side of the firewall, with source IP equal to one of the internal IPs.
  2. **Source Routing Attacks:**  
     In this kind of attack, the attacker specifies the route to be taken by the packet with a hope to fool the firewall.  
     **Prevention:**  
     Firewall can defeat this attack if it discards all the packets that use the option of source routing aka path addressing.
  3. **Tiny Fragment Attacks:**  
     Many times, the size of the IP packet is greater than the maximum size allowed by the underlying network such as Ethernet, Token Ring etc. In such cases, the packet needs to be [fragmented](https://www.geeksforgeeks.org/fragmentation-network-layer/" \t "https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/_blank), so that it can be carried further. The attacker uses this characteristic of TCP/IP protocol. In this kind of attack, the attacker intentionally creates fragments of the original packet and send it to fool the firewall.  
     **Prevention:**  
     Firewall can defeat this attack if it discards all the packets which use the TCP protocol and is fragmented. *Dynamic Packet Filters* allow incoming TCP packets only if they are responses to the outgoing TCP packets.

1. **Application Gateways –**  
   It is also known as **Proxy server**. It works as follows:
   1. **Step-1:** User contacts the application gateway using a TCP/IP application such as HTTP.
   2. **Step-2:** The application gateway asks about the remote host with which the user wants to establish a connection. It also asks for the user id and password that is required to access the services of the application gateway.
   3. **Step-3:** After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.
2. **Stateful Inspection Firewalls –**  
   It is also known as ‘Dynamic Packet Filters’. It keeps track of the state of active connections and uses this information to decide which packets to allow through it, i.e., it adapts itself to the current exchange of information, unlike the normal packet filters/stateless packet filters, which have hardcoded routing rules.
3. **Circuit-Level Gateways –**  
   It works at the **session layer** of the OSI Model. It is the advanced variation of *Application Gateway*. It acts as a virtual connection between the remote host and the internal users by creating a new connection between itself and the remote host. It also changes the source IP address in the packet and puts its own address at the place of source IP address of the packet from end users. This way, the IP addresses of the internal users are hidden and secured from the outside world.

Transection security:-

Security is an essential part of any transaction that takes place over the internet. Customers will lose his/her faith in e-business if its security is compromised. Following are the essential requirements for safe e-payments/transactions −

**Confidentiality** − Information should not be accessible to an unauthorized person. It should not be intercepted during the transmission.

**Integrity** − Information should not be altered during its transmission over the network.

**Availability** − Information should be available wherever and whenever required within a time limit specified.

**Authenticity** − There should be a mechanism to authenticate a user before giving him/her an access to the required information.

**Non-Repudiability** − It is the protection against the denial of order or denial of payment. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly, the recipient of message should not be able to deny the receipt.

**Encryption** − Information should be encrypted and decrypted only by an authorized user.

**Auditability** − Data should be recorded in such a way that it can be audited for integrity requirements.

## Measures to ensure Security

Major security measures are following −

**Encryption** − It is a very effective and practical way to safeguard the data being transmitted over the network. Sender of the information encrypts the data using a secret code and only the specified receiver can decrypt the data using the same or a different secret code.

**Digital Signature** − Digital signature ensures the authenticity of the information. A digital signature is an e-signature authenticated through encryption and password.

**Security Certificates** − Security certificate is a unique digital id used to verify the identity of an individual website or user.

## Security Protocols in Internet

We will discuss here some of the popular protocols used over the internet to ensure secured online transactions.

## Secure Socket Layer (SSL)

It is the most commonly used protocol and is widely used across the industry. It meets following security requirements −

* Authentication
* Encryption
* Integrity
* Non-reputability0

"https://" is to be used for HTTP urls with SSL, where as "http:/" is to be used for HTTP urls without SSL.

### Secure Hypertext Transfer Protocol (SHTTP)

SHTTP extends the HTTP internet protocol with public key encryption, authentication, and digital signature over the internet. Secure HTTP supports multiple security mechanism, providing security to the end-users. SHTTP works by negotiating encryption scheme types used between the client and the server.

### Secure Electronic Transaction

It is a secure protocol developed by MasterCard and Visa in collaboration. Theoretically, it is the best security protocol. It has the following components −

**Card Holder's Digital Wallet Software** − Digital Wallet allows the card holder to make secure purchases online via point and click interface.

**Merchant Software** − This software helps merchants to communicate with potential customers and financial institutions in a secure manner.

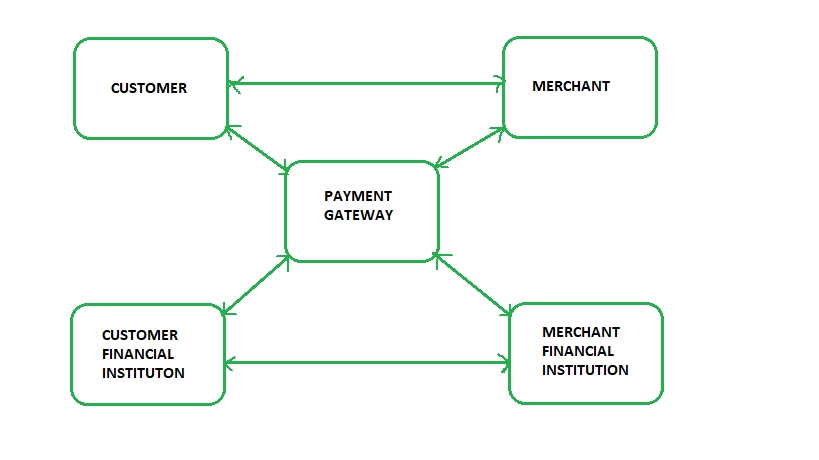
**Payment Gateway Server Software** − Payment gateway provides automatic and standard payment process. It supports the process for merchant's certificate request.

**Certificate Authority Software** − This software is used by financial institutions to issue digital certificates to card holders and merchants, and to enable them to register their account agreements for secure electronic commerce.

# Secure Electronic Transaction (SET) Protocol

**Secure Electronic Transaction** or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied on those payments. It uses different encryption and hashing techniques to secure payments over internet done through credit cards. SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT) and NetScape which provided technology of Secure Socket Layer (SSL).

SET protocol restricts revealing of credit card details to merchants thus keeping hackers and thieves at bay. SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

Before discussing SET further, let’s see a general scenario of electronic transaction, which includes client, payment gateway, client financial institution, merchant and merchant financial institution.  


**Requirements in SET :**  
SET protocol has some requirements to meet, some of the important requirements are :

* It has to provide mutual authentication i.e., customer (or cardholder) authentication by confirming if the customer is intended user or not and merchant authentication.
* It has to keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.
* It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.
* SET also needs to provide interoperability and make use of best security mechanisms.

**Participants in SET :**  
In the general scenario of online transaction, SET includes similar participants:

1. **Cardholder –** customer
2. **Issuer –** customer financial institution
3. **Merchant**
4. **Acquirer –** Merchant financial
5. **Certificate authority –** Authority which follows certain standards and issues certificates(like X.509V3) to all other participants.

#### SET functionalities :

* **Provide Authentication**
  + **Merchant Authentication** – To prevent theft, SET allows customers to check previous relationships between merchant and financial institution. Standard X.509V3 certificates are used for this verification.
  + **Customer / Cardholder Authentication** – SET checks if use of credit card is done by an authorized user or not using X.509V3 certificates.
* **Provide Message Confidentiality** : Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purpose.
* **Provide Message Integrity** : SET doesn’t allow message modification with the help of signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1,

**Dual Signature :**  
The dual signature is a concept introduced with SET, which aims at connecting two information pieces meant for two different receivers :  
**Order Information (OI) for merchant**  
**Payment Information (PI) for bank**

You might think sending them separately is an easy and more secure way, but sending them in a connected form resolves any future dispute possible. Here is the generation of dual signature:  
