**Chapter – 3**

**(Electronic Payment Systems)**

**Class : M.Com.(Final)**

Prof. Vinay Bharti

Dept. of Computer Science

**Introduction:**

bySDVªkWfud Hkqxrku iz.kkyh bysDVªkfud ek/;e }kjk isij jfgr ekSfnzd O;ogkj djus dh lqfo/kk iznku djrh gSA bZ&isesaV vFkkZr~ bysDVªkfud Hkqxrku fof/k ds iz;ksx }kjk O;ogkj ykxrksa] Je ykxrksa] dkxth dk;ksZ esa cgqr cM+h lhek rd deh dh tk ldrh gSA

**,d vkn’kZ bySDVªkWfud Hkqxrku iz.kkyh dh fo’ks”krk,a&**

,d vkn’kZ bySDVªkWfud Hkqxrku iz.kkyh dh fofHkUu fo’ks”krk,a bl izdkj gSa&

1& **lqfo/kktud (Convenience)&**  vkn’kZ bySDVªkWfud Hkqxrku iz.kkyh iz;ksx djus esa ljy o lqxe gksrh gSA le;] iz;kl rFkk vU; fo’ks”k la;a= ftudh vkn’kZ bySDVªkWfud Hkqxrku iz.kkyh eaas O;ogkj djus esa vko’;drk gksrh gS] mudh ykxr ijEijkxr iz.kkyh dh rqyuk esa cgqr de gksrh gSA

2& **lqj{kk (Security)&** ,d vkn’kZ bySDVªkWfud Hkqxrku iz.kkyh esa fd;k x;k Hkqxrku lqjf{kr gksrk gSA blls lEcfU/kr fofHkUu igyqvksa dk o.kZu bl izdkj fd;k x;k gS&

 1& O;kikjh ,oa dszrk bl iz.kkyh ds iz;ksx ds fdlh Hkh izdkjdh vlQyrk o /kks[ks ls gksus okyh gkfu ls cp ldrs gSaA

 mnkgj.k ds fy, Digital Signature, Encryption, SSL SET rFkk vU; lqj{kk izksVksdky ds iz;ksx }kjk vkWuykbu /kks[kksa ls cpk tk ldrk gSA

 2& xzkgd futh lqpukvksa tSls dzsfMV dkMZ dk uEcj] pkj v{kjksa okyk fiu uEcj vkfn ij vukf/kd`r igqWp ls lqj{kk izkIr dj ldrs gSaA

 3& blds vUrxZr ,d O;fDr dh okLrfod igpku ds dqN ek/;e miyC/k gksrs gSA

3& **xksiuh;rk (Secrecy)**& vkn’kZ bySDVªkWfud Hkqxrku iz.kkyh esa xksiuh;rk dks cuk, j[kk tkrk gSA bldk vFkZ ;g gS fd blds vrZxZr fo’oluh;rk iwoZd bySDVªkWfud O;ogkj fd, tk ldrs gSaA fo’oluh;rk ls vfHkizk; dzsrkvksa o fodzsrkvksa ds e/; fd, tkus okys O;ogkj fdlh vU; i{kdkj {kkjk vkadfyr o ns[ks ugh tk ldrsA

4&  **ykxr (Cost)&** vkWuykbu Hkqxrku fof/k ds iz;ksx }kjk xzkgdksa o O;kikfj;ksa dks cgqr de ykxr ogu djuh iM+rh gSA

5& **ekidze.kh;rk (Scalability)&** ekidze.kh;rk fcuk fdlh lsok dks izHkkfor fd, vkWuykbu O;olk; eas u, iz;ksxdrkZvksa dks tksM+rh gSA bldk vFkZ ;g gS fd iz;ksxdrkZvksa dh la[;k c<+kus ds i’pkr~ Hkh Hkqxrku lek/kku iz.kkyh leku O;ogkj ykxr ij lsok iznku djrh gS rFkk O;ogkj xfr Hkh igys ls leku gh gksrh gSA

6& **lkoZHkkSfedrk (Universality)&** ,d vkn’kZ bySDVªkWfud Hkqxrku iz.kkyh eas xzkgdksa o fodszrk ds vyx&vyx ns’k og fHkUu&fHkUu czkmtj lkWW¶Vos;j gksus ds ckotwn Hkh Hkqxrku iz.kkyh ds iz;ksx esa cgqr gh de vojks/k mRiUu gksrs gSA

7& **lw{; Hkqxrku ds fy, lgk;d (Support for Micro Payments)&** lw{; Hkqxrku ls vfHkizk; cgqr de jkf’k ds foRrh; O;ogkjksa ls gS rFkk ;s O;ogkj lkekU;r% vkWuykbu ek/;e ls fd, tkrs gSaA

ijEijk Hkqxrku ds }kjk lw{e Hkqxrkuksa dk fjdkWMZ j[kuk cgqr dfBu gksrk gSA ;s Hkqxrku lkekU;r% uhjl] /khes o eWgxs gksrs gSa ijUrq ,d vkn’kZ bySDVªkWfud Hkqxrku iz.kkyh xzkgdkas dks rhoz xfr] mPp fdLe dh lqfo/kk o de ykxr iznku djrh gS] ftlds ek/;e ls lw{e Hkqxrkuksa dh Hkh ljyrk ls O;oLFkk dh tk ldrh gSA

**Types of Elctronic Payment System:**

* **Credit Card**

A credit card is a thin rectangular plastic card issued by financial institutions, which lets you borrow funds from a pre-approved limit to pay for your purchases. The limit is decided by the institution issuing the card based on your credit score and history. Generally, higher the score and better the history, higher is the limit.

Users can swipe the credit card to make a payment or use it for online transactions. After you [apply for a credit card](https://www.bajajfinserv.in/credit-card), simply make sure that the borrowed amount is repaid within the stipulated time frame to avoid penalty charges. Your credit card details are always secured with the card issuer and you should not share your credit card information with anyone to avoid fraud.

**Uses of Credit Card**

### Take advantage of the grace period

The grace period constitutes the billing period of 30 days along with an additional 15 to 20 days window between the statement generation date and the payment due date. Hence, the total interest-free period can extend up to 50 days.

Making an expensive purchase when the billing period commences thus enables you to take advantage of the full grace period.

### Use the right card for the right purchase

Make sure to learn the use of a credit card if you hold multiple ones. For example, use your [fuel credit card](https://www.bajajfinserv.in/what-is-fuel-credit-card) if you spend a considerable portion of your income on fuel purchases. You can earn accelerated reward points apart from enjoying fuel surcharge waiver.

Contrarily, use your [travel credit card](https://www.bajajfinserv.in/what-is-travel-credit-card) to book flight tickets, hotels, etc. Using the wrong variant will reduce the number of reward points accumulated and simultaneously you benefit less from your credit card.

### Opt for a personal loan during emergencies

Credit cards like the [Bajaj Finserv RBL Bank SuperCard](https://www.bajajfinserv.in/super-card) enable you to convert your unutilised credit limit into an emergency personal loan for an interest-free period of up to 90 days.

### Convert your purchases into EMIs

One of the exceptional uses of a credit card is that you can [convert your purchases into EMIs](https://www.bajajfinserv.in/how-to-convert-credit-card-purchases-into-emis) and repay them affordably.

### Shop online to earn the most reward points

Credit cards give you 2x reward points when you shop online. Learn how to use a credit card online to maximise your rewards.

### Redeem your reward points

You can redeem your reward points get discounts on flight tickets, hotel bookings, etc. These points can get you exclusive shopping vouchers recharge vouchers and even cashback at times.

**Process of using Credit Cards**

The major steps in Credit Card Transactions are shown in figure.



Steps are:

1. Issue a credit card on request to a potential cardholder.The card is activated as soon as the cardholder calls the bank for initiation.
2. The cardholder presence his or her credit card information to a merchantwhenever he or she needs to pay for a product or service.
3. The merchant validates the customer’s identity as the owner of the credit cardaccount. For this purpose, the merchant ask for approval from the card brand company.Figure shows a flowchart that explain the credit card transaction.
4. The card brand company return the credit card data, change authentication and authorization to the merchant. The transaction is paid by credit . The merchant keeps a sales slip.
5. The merchant submits the sales slip to the acquiring bank and pays service charges. Thus is Called a capturing process.
6. The acquiring bank request the card brand to clear for the credit card amount and gets paid.
7. Now the card brands for clearance to the issue bank.The amount is transferred from issuer to card brand.

In the conventional credit card system, the process just described is only partially automated. However, the entire process must by fully automated on the internet in a secure manner

.

* **Debit Card**

A **debit card** (also known as a **bank card**, **plastic card** or **check card**) is a [plastic](https://en.wikipedia.org/wiki/ISO/IEC_7812) [payment card](https://en.wikipedia.org/wiki/Payment_card) that can be used instead of [cash](https://en.wikipedia.org/wiki/Cash) when making purchases. It is similar to a [credit card](https://en.wikipedia.org/wiki/Credit_card), but unlike a credit card, the money is immediately transferred directly from the cardholder's [bank account](https://en.wikipedia.org/wiki/Bank_account) when performing any transaction.

Some cards might carry a [stored value](https://en.wikipedia.org/wiki/Stored-value_card) with which a payment is made, while most relay a message to the cardholder's bank to withdraw funds from a payer's designated bank account. In some cases, the [primary account number](https://en.wikipedia.org/wiki/Primary_account_number) is assigned exclusively for use on the Internet and there is no physical card.

## Precautions With a Debit Card

One of the biggest precautions you need to take with your debit card is to make sure that it or the information on it is not stolen. If your card is physically stolen, you need to call the bank immediately and cancel the card. Criminals might hack a website and steal the card information and then use it to make purchases online. Your bank may have sent you a new debit card at some point because there was a data breach at a merchant. If you find unauthorized transactions in your account, you need to call the bank immediately to find out what happened.

Another way that criminals are getting the information is through card skimming. The person can either swipe your card through the machine themselves (this happens at restaurants or other places where they take your card from you momentarily) or they can attach a skimmer to a machine where you use your card (like an ATM, vending machine, or RedBox). The skimmers are very small and blend in well. They can be difficult to spot. However, if one of these looks off to you, especially where you swipe the card, you should likely use a different ATM or vending machine. It is important to check your account regularly and watch out for unauthorized transactions, because the sooner you spot the problem, the easier it will be to resolve.

**Difference between Debit Card and Credit Card**

|  |  |
| --- | --- |
| **Credit Card** | **Debit Card** |
| Credit cards allow the cardholders to purchase goods and services on credit and pay it back over time | In case of a debit card,‭ ‬the amount is instantly deducted from your bank account |
| You have the option to convert your credit card purchases into EMIs | No credit facility is available,‭ ‬as you pay instantly from your own funds |
| Provides better security in case of faulty transactions | Provides less security in case of faulty transactions |
| Typically offered with joining and annual fees | Typically issued free with your savings account |
| The penalty is charged on non-payment or late payment of your credit card dues | Penalty charges are not applicable in case of debit cards |

* **Smart Card**

A smart card is a physical card that has an [embedded](https://internetofthingsagenda.techtarget.com/definition/embedded-system) integrated chip that acts as a security token. Smart cards are typically the same size as a driver's license or credit card and can be made out of metal or plastic. They connect to a reader either by direct physical contact (also known as [chip and dip](https://whatis.techtarget.com/definition/card-dipping-EMV-card-dipping)) or through a short-range wireless connectivity standard such as radio-frequency identification ([RFID](https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification)) or near-field communication ([NFC](https://searchmobilecomputing.techtarget.com/definition/Near-Field-Communication)).

The chip on a smart card can be either a [microcontroller](https://internetofthingsagenda.techtarget.com/definition/microcontroller) or an embedded memory chip. Smart cards are designed to be tamper-resistant and use encryption to provide protection for in-memory information. Those cards with microcontroller chips can perform on-card processing functions and can manipulate information in the chip's memory.

Smart cards are used for a variety of applications, though most commonly are used for credit cards and other payment cards. Distribution of smart cards in recent years has been driven by the payment card industry's move to support smart cards for the [EMV payment card](https://whatis.techtarget.com/definition/EMV-card) standard. Smart cards capable of short-range wireless connectivity can also be used for contactless payment systems; they can also be used as tokens for multifactor authentication.

International standards and specifications cover smart card technology, with some focused on industry-specific applications. In the United States, smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) championed by the Smartcard Alliance.

The first mass *use* of smart cards was the Télécarte, a telephone card for payment in French pay phones which launched in 1983. Smart cards are now ubiquitous and have largely replaced [magnetic stripe](https://whatis.techtarget.com/definition/magnetic-stripe-reader-magstripe-reader) (also known as "mag stripe") card technology, which only has a capacity of 300 bytes of non-rewriteable memory and no processing capability.

**How smart cards work**

Smart card microprocessors or memory chips exchange data with card readers and other systems over a serial interface. The smart card itself is powered by an external source, usually the smart card reader. A smart card communicates with readers either via direct physical contact or using a short-range wireless connectivity standard such as RFID or NFC. The card reader then passes data from the smart card to its intended destination, usually a payment or authentication system connected to the smart card reader over a network connection.

### Uses of smart cards

Smart cards are generally used in applications that must deliver fast, secure transactions and protect personal information such as credit cards and other types of payment cards, corporate and government identification cards and transit fare payment cards. Smart cards are also sometimes used to function as documents such as electronic passports and visas.

Smart cards are often designed to be used with a PIN, for example, when they are used as debit or ATM cards. Organizations also use smart cards for security purposes; in addition to their use as multifactor authentication tokens, the cards can also be used for authenticating [single sign-on](https://searchsecurity.techtarget.com/definition/single-sign-on) users.

### Types of smart cards

Smart cards can be categorized on different criteria including by how the card reads and writes data, by the type of chip implanted in the card and by the capabilities of that chip. Some of the different of types of smart cards include:

* **Contact smart cards** are the most common type of smart card. Contact smart cards are inserted into a smart card reader that has a direct connection to a conductive contact plate on the surface of the card. Commands, data and card status are transmitted over these physical contact points.
* **Contactless smart cards** require only close proximity to a card reader to be read; no direct contact is necessary for the card to function. The card and the reader are both equipped with antennae and communicate using radio frequencies over the contactless link. A contactless smart card functions by being put near the reader to be read.
* **Dual-interface cards** are equipped with both contactless and contact interfaces. This type of card enables secure access to the smart card's chip with either the contactless or contact smart card interfaces.
* **Hybrid smart cards** contain more than one smart card technology. For example, a hybrid smart card might have one embedded processor chip that is accessed through a contact reader as well as an RFID-enabled chip used for proximity connection. The two different chips may be used for different applications linked to a single smart card, as when the proximity chip is used for physical access to restricted areas while the contact smart card chip is used for single sign-on authentication.
* **Memory smart cards** contain memory chips only and can only store, read and write data to the chip; the data on memory smart cards can be over-written or modified, but the card itself is not programmable so data can't be processed or modified programmatically. Memory smart cards can be read-only and used to store data such as a PIN, password or public key; they can also be read-write and used to write or update user data. Memory smart cards can be configured to be rechargeable or disposable, in which case they contain data that can only be used once or for a limited time before being updated or discarded.
* **Microprocessor smart cards** have a microprocessor embedded onto the chip in addition to memory blocks. A microprocessor card may also incorporate specific sections of files where each file is associated with a specific function. The data in the files and the memory allocation are managed with a smart card operating system. This type of card can be used for more than one function and is usually designed to enable adding, deleting and otherwise manipulating data in memory.