**UNIT II**

**UNIT-2 Application security (Database, E-mail and Internet), Data Security ConsiderationsBackups, Archival Storage and Disposal of Data, Security Technology-Firewall and VPNs, Intrusion Detection, Access Control. Security Threats -Viruses, Worms, Trojan Horse, Bombs, Trapdoors, Spoofs, E-mail viruses, Macro viruses, Malicious Software, Network and Denial of Services Attack, Security Threats to E-Commerce- Electronic Payment System, e-Cash,**

**Credit/Debit Cards. Digital Signature, public Key Cryptography.**

# Application Security in DBMS

**Application security denotes the security at the application level to prevent the stealing or capturing of data or code inside the application. It also includes the security measurements made during the advancement and design of applications, as well as techniques and methods for protecting the applications whenever. Application security is the discipline of processes, tools, and works on planning to protect applications from dangers all through the whole application lifecycle. It can assist associations in protecting a wide range of applications (like inheritance, work area, web, portable) used by partners including clients, colleagues, and representatives.**

**Types of Application Security:**

* **Authentication: Authentication is a method of ensuring that only authorized users. A weakness known as cross-site scripting (XSS) permits an attacker to introduce clientside code into a site page. The attacker gets direct access to the user’s data.rs to have access of controlling the application. Authentication methods confirm that the user is who they guarantee to be. While signing into an application, this can be performed by requiring the user to supply a username and password. There is also multi-level authentication which ensures maximum security, for example, something you know (a password), something you have (a cell phone), and something you are (a biometric).**
* **Authorization: After authentication, the user is allowed to access and use the application. The application of the user is only validated after comparing the identification of the user to approve the access, thus authentication has to be always before the authorization step.**
* **Encryption: After the verification and authorization of the user while using the application other security protocols can protect the data from threats. Encryption is done to keep sensitive data safe while flowing from end-user to cloud in cloud-based applications.**
* **Logging: Assuming a security break happens in an application, logging can help with figuring out who accessed the data and how it happened. Application log records monitor who accessed and what portions of the application have been accessed.**
* **Application Security Testing: A strategy that guarantees that these security controls are working actually.**

**What is Email Security?**

**Basically, Email security refers to the steps where we protect the email messages and the information that they contain from unauthorized access, and damage. It involves ensuring the confidentiality, integrity, and availability of email messages, as well as safeguarding against phishing attacks, spam, viruses, and another form of malware. It can be achieved through a combination of technical and non-technical measures.**

**Some standard technical measures include the encryption of email messages to protect their contents, the use of digital signatures to verify the authenticity of the sender, and email filtering systems to block unwanted emails and malware, and the non-technical measures may include training employees on how to recognize and respond to phishing attacks and other email security threats, establishing policies and procedures for email use and management, and conducting regular security audits to identify and address vulnerabilities.**

**Why is email security important?**

* **Protection Against Cyberattacks: Email is a top goal for cybercriminals. Malware, phishing attacks, and other threats often arrive via email. In fact, 94% of malware is delivered through email channels1. By implementing robust email security measures, organizations can defend against these threats.**
* **Reducing Risk: Cybersecurity incidents can have devastating consequences, including financial losses, operational disruptions, and damage to an organization’s reputation. Effective email security helps protect your brand, reputation, and bottom line.**
* **Compliance: Email security ensures compliance with data protection laws like GDPR and HIPAA. By safeguarding sensitive information, organizations avoid legal fines and other intangible costs associated with cyberattacks.**

**GDPR stands for General Data Protection Regulation, and HIPAA stands for Health Insurance Portability and Accountability Act. Both are regulations that require organizations to protect and manage users' personal data.**

* **Productivity Enhancement: With email security in place, disruptions caused by threats like phishing emails are minimized. This allows organizations to focus more on business growth and less on handling security incidents.**

# Benefits of Email Security

* **Shielding Against Phishing and Spoofing Attacks: Email security isn’t just about tech jargon; it’s like having a digital bodyguard. It helps spot and tackle threats like phishing or spoofing. These sneaky attacks can lead to serious breaches and even unleash malware or other nasty viruses.**
* **Locking Down Data: Think of email encryption as a virtual vault. It keeps sensitive info—like credit card numbers, bank accounts, and employee details—safe from prying eyes. No more accidental leaks or costly data breaches!**
* **Whispers Only: Secure email encryption ensures that only the right people get the message. It’s like passing a secret note in class—except the teacher won’t intercept it.**

**Your confidential content stays confidential.**

* **Spotting the Bad Apples: Email security acts like a spam filter on steroids. It sniffs out malicious or spammy emails that might sneak past regular defenses. No more falling for those “You’ve won a million dollars!” scams!**
* **Top-Secret Protection: Imagine your company’s secrets—intellectual property, financial records, and classified info—wrapped in a digital force field. Email security shields them from cyber villains like hackers and cybercriminals.**
* **Real-Time Guardian: Zero-day exploits? Not on our watch! Email security solutions provide real-time protection. It’s like having a superhero squad that fights off malware and spam before they even knock on your inbox.**
* **Locking Up Identity Theft: Email encryption keeps attackers from swiping your login credentials or personal data. No more compromised accounts or identity theft nightmares.**

**What is Network Security?**

**Any action intended to safeguard the integrity and usefulness of your data and network is known as network security. In other words, Network security is defined as the activity created to protect the integrity of your network and data.**

**Network security is the practice of protecting a computer network from unauthorized access, misuse, or attacks. It involves using tools, technologies, and policies to ensure that data traveling over the network is safe and secure, keeping sensitive information away from hackers and other threats.**



# Data Security Consideration

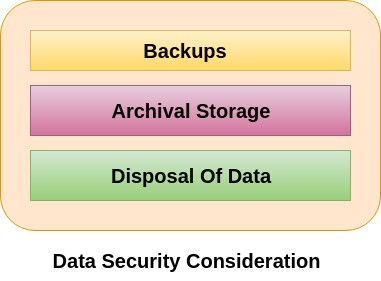
**Data security is the protection of programs and data in computers and communication systems against unauthorized access, modification, destruction, disclosure or transfer whether accidental or intentional by building physical arrangements and software checks. It refers to the right of individuals or organizations to deny or restrict the collection and use of information about unauthorized access. Data security requires system managers to reduce unauthorized access to the systems by building physical arrangements and software checks.**

**Data security uses various methods to make sure that the data is correct, original, kept confidentially and is safe. It includes-**

* **Ensuring the integrity of data. o Ensuring the privacy of the data. o Prevent the loss or destruction of data.**

**Data security consideration involves the protection of data against unauthorized access, modification, destruction, loss, disclosure or transfer whether accidental or intentional. Some of the important data security considerations are described below:**

**Backups**



**Data backup refers to save additional copies of our data in separate physical or cloud locations from data files in storage. It is essential for us to keep secure, store, and backup our data on a regular basis. Securing of the data will help us to prevent from-**

* **Accidental or malicious damage/modification to data.**
* **Theft of valuable information.**
* **Breach of confidentiality agreements and privacy laws.**
* **Premature release of data which can avoid intellectual properties claims. o Release before data have been checked for authenticity and accuracy.**

**Keeping reliable and regular backups of our data protects against the risk of damage or loss due to power failure, hardware failure, software or media faults, viruses or hacking, or even human errors.**

**To use the Backup 3-2-1 Rule is very popular. This rule includes:**

* **Three copies of our data o Two different formats, i.e., hard drive+tape backup or DVD (short term)+flash drive o One off-site backup, i.e., have two physical backups and one in the cloud**

## Some important backup options are as follows-

1. **Hard drives - personal or office computer**
2. **Departmental or institution server**
3. **External hard drives**
4. **Tape backups**
5. **Discipline-specific repositories**
6. **University Archives**
7. **Cloud storage**

**Some of the top considerations for implementing secure backup and recovery are-**

1. **Authentication of the users and backup clients to the backup server.**
2. **Role-based access control lists for all backup and recovery operations.**
3. **Data encryption options for both transmission and the storage.**
4. **Flexibility in choosing encryption and authentication algorithms.**
5. **Backup of a remote client to the centralized location behind firewalls.**
6. **Backup and recovery of a client running Security-Enhanced Linux (SELinux).**
7. **Using best practices to write secure software.**

## Archival Storage

**Data archiving is the process of retaining or keeping of data at a secure place for long-term storage. The data might be stored in safe locations so that it can be used whenever it is required. The archive data is still essential to the organization and may be needed for future reference. Also, data archives are indexed and have search capabilities so that the files and parts of files can be easily located and retrieved. The Data archival serve as a way of reducing primary storage consumption of data and its related costs.**

**Data archival is different from data backup in the sense that data backups created copies of data and used as a data recovery mechanism to restore data in the event when it is corrupted or destroyed. On the other hand, data archives protect the older information that is not needed in day-to-day operations but may have to be accessed occasionally.**

**Data archives may have many different forms. It can be stored as Online, offline, or cloud storage-**

**o Online data storage places archive data onto disk systems where it is readily accessible. o Offline data storage places archive data onto the tape or other removable media using data archiving software. Because tape can be removed and consumes less power than disk systems. o Cloud storage is also another possible archive target. For example, Amazon Glacier is designed for data archiving. Cloud storage is inexpensive, but its costs can grow over time as more data is added to the cloud archive.**

**The following list of considerations will help us to improve the long-term usefulness of our archives:**

1. **Storage medium**
2. **Storage device**
3. **Revisiting old archives**
4. **Data usability**
5. **Selective archiving**
6. **Space considerations**
7. **Online vs. offline storage**

### Storage medium

**The first thing is to what storage medium we use for archives. The archived data will be stored for long periods of time, so we must need to choose the type of media that will be lost as long as our retention policy dictates.**

### Storage device

**This consideration takes into account about the storage device we are using for our archives which will be accessible in a few years. There is no way to predict which types of storage devices will stand the best. So, it is essential to try to pick those devices that have the best chance of being supported over the long term.**

### Revisiting old archives

**Since we know our archive policies and the storage mechanisms we use for archiving data would change over time. So we have to review our archived data at least once a year to see that if anything needs to be migrated into a different storage medium.**

**For example, about ten years ago, we used Zip drives for archival then we had transferred all of my archives to CD. But in today?s, we store most of our archives on DVD. Since modern DVD drives can also read CDs, so we haven't needed to move our extremely old archives off CD onto DVD.**

### Data usability

**In this consideration, we have seen one major problem in the real world is archived data which is in an obsolete format.**

**For example, a few years ago, document files that had been archived in the early 1990s were created by an application known as PFS Write. The PFS Write file format was supported in the late 80s and early 90s, but today, there are not any applications that can read that files. To avoid this situation, it might be helpful to archive not only the data but also copies the installation media for the applications that created the data.**

### Selective archiving

**In this consideration, we have to sure about what should be archived. That means we will archive only a selective part of data because not all data is equally important.**

### Space considerations

**If our archives become huge, we must plan for the long-term retention of all our data. If we are archiving our data to removable media, capacity planning might be simple which makes sure that there is a free space in the vault to hold all of those tapes, and it makes sure that there is a room in our IT budget to continue purchasing tapes.**

### Online vs. offline storage

**In this consideration, we have to decide whether to store our archives online (on a dedicated archive server) or offline (on removable media). Both methods of archival contain advantages and disadvantages. Storing of data online keeps the data easily accessible. But keeping data online may be vulnerable to theft, tampering, corruption, etc. Offline storage enables us to store an unlimited amount of data, but it is not readily accessible.**

## Disposal of Data

**Data destruction or disposal of data is the method of destroying data which is stored on tapes, hard disks and other electronic media so that it is completely unreadable, unusable and inaccessible for unauthorized purposes. It also ensures that the organization retains records of data for as long as they are needed. When it is no longer required, appropriately destroys them or disposes of that data in some other way, for example, by transfer to an archives service.**

**The managed process of data disposal has some essential benefits- o It avoids the unnecessary storage costs incurred by using office or server space in maintaining records which is no longer needed by the organization.**

* **Finding and retrieving information is easier and quicker because there is less to search.**

**The disposal of data usually takes place as part of the normal records management process. There are two essential circumstances in which the destruction of data need to be handled as an addition to this process-**

* **The quantity of a legacy record requires attention. o The functions are being transferred to another authority and disposal of data records becomes part of the change process.**

**The following list of considerations will help us for the secure disposal of data-**

1. **Eliminate access**
2. **Destroy the data**
3. **Destroy the device**
4. **Keep the record of which systems have been decommissioned**
5. **Keep careful records**
6. **Eliminate potential clues**
7. **Keep systems secure until disposal**

### Eliminate access

**In this consideration, we have to ensure that eliminating access account does not have any rights to re access the disposed of data again.**

### Destroy the Data

**In this consideration, there is not necessary to remove data from storage media will be safe. Even these days reformatting or repartitioning a drive to "erase" the data that it stores is not good enough. Today's many tools available which can help us to delete files more securely. To encrypt the data on the drive before performing any deletion can help us to make data more difficult to recover later.**

### Destroy the device

**In the most cases, storage media need to be physically destroyed to ensure that our sensitive data is not leaked to whoever gets the drives next. In such cases, we should not destroy them itself. To do this, there should be experts who can make probably a lot better at safely and effectively rendering any data on our drives unrecoverable. If we can't trust this to an outsider agency that specializes in the secure destruction of storage devices, we should have a specialized team within our organization who has the same equipment and skills as outside contractors.**

### Keep the record of which systems have been decommissioned

**In this, we have to make sure that the storage media has been fully decommissioned securely and they do not consist of something easily misplaced or overlooked. It is best if storage media that have not been fully decommissioned are kept in a specific location, while decommissioned equipment placed somewhere else so that it will help us to avoid making mistakes.**

### Keep careful records

**In this consideration, it is necessary to keep the record of whoever is responsible for decommissioning a storage media. If more than one person is assigned for such responsibility, he should sign off after the completion of the decommissioning process. So that, if something happened wrong, we know who to talk to find out what happened and how bad the mistake is. Eliminate potential clues**

**In this consideration, we have to clear the configuration settings from networking equipment. We do this because it can provide crucial clues to a security cracker to break into our network and the systems that reside on it.**

### Keep system secure until disposal of data

**In this consideration, we should have to make clear guidelines for who should have access to the equipment in need of secure disposal. It will be better to ensure that nobody should have access authentication to it before disposal of data won't get his or her hands on it.**

**Security technology-firewall and VPNs,**

## Firewall

**Firewalls and Virtual Private Networks (VPNs) are two distinct security technologies that serve different purposes in protecting a network. While they can be used separately, they are often employed together to provide a robust defence against various threats. Firewalls**

**A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its primary functions are:**

* **Blocking unauthorized access to or from a private network**
* **Filtering traffic based on source and destination IP addresses, ports, and protocols**
* **Detecting and preventing malicious traffic patterns, such as denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks**

**Firewalls can be implemented as software, hardware, or a combination of both.**

**VPNs**

**A VPN creates a secure and encrypted “tunnel” between a device and a VPN server, allowing users to access a network as if they were directly connected to it. VPNs provide:**

* **Encryption of data in transit, protecting against eavesdropping and interception**
* **Authentication of users and devices, ensuring only authorized parties can access the network • Masking of IP addresses, making it difficult for attackers to identify and target specific devices**

**VPNs are commonly used for remote access, allowing employees to securely connect to a company network from anywhere.**

**Combining Firewalls and VPNs**

**When used together, firewalls and VPNs provide a multi-layered defence:**

* **Firewalls control incoming and outgoing traffic at the network perimeter, blocking unauthorized access and malicious traffic.**
* **VPNs encrypt and authenticate traffic within the network, ensuring secure communication between devices and servers. By combining these technologies, organizations can:**
* **Protect against a wide range of threats, including hacking, data theft, and malware**
* **Ensure network resources are available and accessible only to authorized users**
* **Comply with regulatory requirements and industry standards for network security In summary, firewalls and VPNs are complementary security technologies that work together to provide robust network protection. Firewalls focus on controlling network traffic at the perimeter, while VPNs ensure secure communication within the network.**

### Intrusion Detection

**An Intrusion Detection System (IDS) is a security tool that monitors computer networks or systems for malicious activities or policy violations. Its primary function is to detect and alert administrators to unauthorized access, potential threats, and abnormal activities by analyzing network traffic.**

**Key Characteristics:**

* **Monitors network traffic for suspicious activity**
* **Sends alerts when malicious activity is detected**
* **Analyzes traffic to identify anomalies and policy violations**
* **Typically reports or collects detected incidents centrally using a Security Information and Event Management (SIEM) system Functions:**
* **Anomaly detection: Identifies unusual patterns or behavior in network traffic**
* **Reporting: Provides alerts and notifications to administrators of detected incidents**
* **Some IDS systems may also take action when malicious activity or anomalous traffic is detected**

**In summary, an Intrusion Detection System is a critical security component that helps protect networks and systems from unauthorized access and malicious activities by monitoring traffic, detecting anomalies, and alerting administrators to take action.**

### Access control

**Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that** [**minimizes risk**](https://www.techtarget.com/searchstorage/tip/Prevent-the-storage-and-data-security-risks-of-remote-work) **to the business or organization.**

**There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.**

**To secure a facility, organizations use electronic access control systems that rely on user credentials, access card readers, auditing and reports to track employee access to restricted business locations and proprietary areas, such as data centers. Some of these systems incorporate access control panels to restrict entry to rooms and buildings, as well as alarms and lockdown capabilities, to prevent unauthorized access or operations.**

**Logical access control systems perform identification** [**authentication**](https://www.techtarget.com/searchsecurity/definition/authentication) **and Authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers,** [**biometric**](https://www.techtarget.com/searchsecurity/definition/biometrics) **scans, security tokens or other** [**authentication factors.**](https://www.techtarget.com/searchsecurity/definition/authentication-factor) **Multifactor authentication (**[**MFA)**](https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA)**, which requires two or more authentication factors, is often an important part of a layered defence to protect access control systems.**

**What are Cybersecurity Threats?**

[**Cybersecurity**](https://www.imperva.com/learn/application-security/cyber-security/) **threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems. Common categories of cyber threats include malware, social engineering, man in the middle (MitM) attacks, denial of service (DoS), and injection attacks—we describe each of these categories in more detail below.**

**Cyber threats can originate from a variety of sources, from hostile nation states and terrorist groups to individual hackers, to trusted individuals like employees or contractors, who abuse their privileges to perform malicious acts.**

#### Common Sources of Cyber Threats

**Here are several common sources of cyber threats against organizations:**

* **Nation states—hostile countries can launch cyber-attacks against local companies and institutions, aiming to interfere with communications, cause disorder, and inflict damage.**
* **Terrorist organizations—terrorists conduct cyber-attacks aimed at destroying or abusing critical infrastructure, threaten national security, disrupt economies, and cause bodily harm to citizens.**
* **Criminal groups—organized groups of hackers aim to break into computing systems for economic benefit. These groups use phishing, spam, spyware and malware for extortion, theft of private information, and online scams.**
* **Hackers—individual hackers target organizations using a variety of attack techniques. They are usually motivated by personal gain, revenge, financial gain, or political activity. Hackers often develop new threats, to advance their criminal ability and improve their personal standing in the hacker community.**
* **Malicious insiders—an employee who has legitimate access to company assets, and abuses their privileges to steal information or damage computing systems for economic or personal gain. Insiders may be employees, contractors, suppliers, or partners of the target organization. They can also be outsiders who have compromised a privileged account and are impersonating its owner.**

**Definition of Virus**

**A computer virus is a malicious software program loaded onto a user’s computer without the user’s knowledge and performs malicious actions.**

**A virus is a small piece of software that piggybacks on real programs in order to get Executed.**

**Once it’s running, it spreads by inserting copies of itself into other executable code or Documents.**

**Characteristics of a Virus Viruses have four essential characteristics.**

**SELF REPLICATION: First, viruses are notable for the ability to replicate itself to infect computers, much like its biological counterpart. By replicating itself it is able to spread across computer systems and networks to infect as much as it possibly can.**

**EXECUTABLE PATH: Second, before the virus can do anything, it must be executed. If it cannot be executed, it is harmless. To get itself to replicate it hitches a ride by attaching itself to an executable program. It has to modify the program involved to also execute the virus code. The virus is usually attached to a common executable such as the operating system, which is automatically executed on startup. It may also attach itself to a commonly executed file that a specific company may use.**

**SIDE EFFECTS: Third, viruses do not just contain self-replicating code; they also contain what is called a payload. The payload is similar to a warhead on a missile; it is the side-effect of the virus. The payload has the potential to be malicious, but it does not have to be.**

**DISGUISE: Lastly, the virus will be able to disguise itself before it is noticed by its sideeffects. There are two methods of disguise, encryption and interrupt interception.**

**What Viruses May Do to a Computer?**

**•Delete files.**

**•Varies messages in files or on programs.**

**•Changes volume label.**

**•Randomly overwrites sectors on the hard disk.**

**•Marks clusters as bad in the FAT (file allocation table) •Replaces the MBR (master boot record ) with own code.**

**•Create more than one partition.**

**•Causes cross-linked files.**

**•Causes a "sector not found" error.**

**•Cause the system to run slow.**

**•A directory may be displayed as garbage.**

**•Directory order may be modified so files, such as COM files, will start at the beginning of the directory.**

**•Causes keyboard keys to be remapped.**

**•Functions slower than normal**

**•Responds slowly and freezes often**

**•Restarts itself often**

**•See uncommon error messages, distorted menus, and dialog boxes**

**•Notice applications fail to work correctly**

**•Fail to print correctly**

### Types of Computer Virus

1. **Worm**
2. **Trojan Horse**
3. **Time Bomb**
4. **Logical Bomb**
5. **Trapdoors**
6. **Spoofs**
7. **E-mail viruses**
8. **Macro viruses**

**A worm is also a destructive program that fills a computer system with self-replicating information, clogging the system so that its operations are slowed down or stopped**

**Trojan Horse is a destructive program. It usually pretends as computer games or application software. If executed, computer system will be damaged.**

**Time bomb is a virus program that performs an activity on a particular date**

**Logical bomb is a destructive program that performs an activity when a certain action has occurred.**

**Trapdoors In computer security, a trapdoor can also be a defect in computer code that allows malicious actors to access valuable information. For example, a trapdoor could allow someone to read cryptographically protected information by using their knowledge of weaknesses in the algorithm used to protect the data.**

**Spoofs Spoofing is a sort of fraud in which someone or something forges the sender’s identity and poses as a reputable source, business, colleague, or other trusted contact in order to obtain personal information, acquire money, spread malware, or steal data.**

**E-mail viruses an email** [**virus**](https://www.techtarget.com/searchsecurity/definition/virus) **consists of malicious code distributed in email messages to infect one or more devices. This malicious code can be activated in numerous ways: when the email recipient clicks on an infected link within the message, opens an infected attachment or interacts with the message in some other way.**

**Email viruses often spread by causing the malicious message to be sent to everyone in the original victim's address book.**

**Simply put, an email virus is a malicious code or a link to malicious code sent via email. The virus has the ability to replicate itself so it can quickly spread from one device to another. Thus, an email virus can not only infect the victim's computer, but it can also infect the computers of everyone in the victim's address book or those sharing the same network.**

**There are three primary ways an email virus can infect a victim's email and computer: 1. via a** [**phishing**](https://www.techtarget.com/searchsecurity/definition/phishing) **email**

1. **included in an attachment**
2. **embedded within the email body**

**Macro viruses a malicious code specifically designed by the hacker or attacker using the macro language (A language that is used to build applications such as Microsoft Word, Excel, or PowerPoint). Macro viruses attach themselves to documents and spreadsheets, and when these files are opened or edited, they infect other documents as well. The dangerous thing about macro viruses is that they can infect any computer, regardless of the operating system it runs on. This means that whether your computer is running Windows, macOS, or Linux, it is vulnerable to a macro virus attack.**

### Denial of Service

**Denial of Service (DoS) is a cyber-attack on an individual Computer or Website with the intent to deny services to intended users. Their purpose is to disrupt an organization’s network operations by denying access to its users. Denial of service is typically accomplished by flooding the targeted machine or resource with surplus requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. For example, if a bank website can handle 10 people a second by clicking the Login button, an attacker only has to send 10 fake requests per second to make it so no legitimate users can log in. DoS attacks exploit various weaknesses in computer network technologies. They may target servers, network routers, or network communication links. They can cause computers and routers to crash and links to bog down. The most famous DoS technique is the Ping of Death. The Ping of Death attack works by generating and sending special network messages (specifically, ICMP packets of non-standard sizes) that cause problems for systems that receive them. In the early days of the Web, this attack could cause unprotected Internet servers to crash quickly. It is strongly recommended to try all described activities on virtual machines rather than in your working environment.**

**What are the 4 types of attacks in network security?**

**While there are countless types of attacks used every day, you could realistically break the majority of them down into the following 4 categories:**

1. **Malware Attacks: Malware stands for malicious software. This encompasses a wide range of harmful programs that can infiltrate a network through vulnerabilities. Malware can steal data, corrupt files, disrupt operations, or even take control of systems. Examples include viruses, worms, Trojan horses, ransomware, and spyware.**

1. **Phishing Attacks: Phishing attacks attempt to trick users into revealing sensitive information, such as usernames, passwords, or credit card details. Phishers often use emails or fraudulent websites that appear legitimate. Once a user enters their information, the attacker can steal it and misuse it.**

1. **Password Attacks: These attacks target passwords to gain unauthorized access to a network or system. Hackers can employ various techniques to crack passwords, including brute-force attacks (trying every possible combination), dictionary attacks (using common words and phrases), and social engineering (tricking users into revealing their passwords).**

1. **Denial-of-Service (DoS) Attacks: DoS attacks aim to overwhelm a network or system with traffic, making it unavailable to legitimate users. Attackers can flood the target with a massive amount of data requests, causing it to crash or become unresponsive. This can disrupt critical operations and cause significant financial losses.**

### E-Commerce website

**The E-Commerce website contains confidential information provided by customers, such as their password, contact details, and credit card details but. when concentrating on commercial deals among organizations and individuals demanding a selective information system under the guarantee of the firm, it accepts the form of e-business. E-commerce is broken into six main categories, which are given below:**

1. **Business to Business E-commerce (B2B E-commerce)**
2. **Business to Consumer E-commerce (B2C E-commerce)**
3. **Consumer to Business E-commerce (C2B E-commerce)**
4. **Consumer to Consumer E-commerce (C2C E-commerce)**
5. **Business to Government( B2G E-commerce)**
6. **Government to Business (G2B E-commerce)**

**These are explained as following below.**

1. **Business to Business E-commerce (B2B E-commerce):**

**In Business-to-Business E-commerce, both participants are businesses. As a result, the volume and value of B2B e-commerce can be huge. B2B stands for business to business. It consists of the largest form of e-commerce. This model defines that buyer and seller are two different entities. It is similar to a manufacturer issuing goods to the retailer or wholesaler.**

1. **Business to Consumer E-commerce (B2C E-commerce):**

**It is a model taking business and consumers interaction. Online business interaction sells to individuals. The basic concept of the model is to sell the product online to the consumers. B2C is the indirect trade between the company and consumer. It provides direct selling online and B2C stands for business to consumer as the name suggests. 3. Consumer to Business E-commerce (C2B E-commerce):**

**A consumer posts his project with a set budget online and within hour company review the consumer’s requirement and bid on the project. The consumer reviews the bid and selects the company that will complete the project. Elance company empowers consumers around the world by providing a meeting ground and a platform for such transactions.**

1. **Consumer to Consumer E-commerce (C2C E-commerce):**

**C2C stands for the consumer to consumer as the name suggests. Though there are no major parties need parties will not fulfill the transaction without the program. That is because it is the most popular platform that enables the consumer to sell to other consumers.**

1. **Business to Government( B2G E-commerce):**

**The B2G model of E-commerce is a model in which businesses sell products and services directly to the government or government agencies. This model provides a way for businesses to bid on government projects or products that government might purchase or need from their organizations. Business to Government activities is increasing.**

1. **Government to Business (G2B E-commerce): The government to Business model involves transactions between a government and business organizations. For Example, the government plans to build a flyover. For this, the government requests for tenders from various contractors through the website. Such government websites support auctions, tenders, and application submission functionalities.**

**Security Threats to E-commerce:**

**E-commerce online system represents the exchange of goods and services over the Internet and also e-commerce also applies to business-to-business transaction. For Example, between manufacturer and supplier or distributor. E-commerce system is also relevant for the service security, for example, online banking and brokerage services allow the customer to retrieve bank statement online, transfer funds pay credit card bills, etc.**

**There are many threats which are given below:**

* **Disclosure of secret data.**
* **Passing or demolition of data.**
* **Mutation of data.**
* **Denial of services.**
* **Inaccuracy in software. • Repudiation.**

**Electronic Payment System: Types, Advantages, Disadvantages and Regulatory Bodies An Electronic Payment System is defined as a mode of payment over an electronic network, such as the Internet. The Indian economy has developed at a rapid pace since the growth of ecommerce, electronic payments, and digital payments have gone a long way. Electronic payments have been rising since the implementation of demonetization and will continue to do so with the current government ensuring that these types of payments are promoted.**

**Geeky Takeaways:**

* **Electronic Payment System allows customers to pay for goods and services electronically without the use of cheques or cash.**
* **Businesses need a strong and secure electronic payment system in online dealings.**
* **Electronic Payment System is regulated in India by the RBI.**
* **The system is safe, speedy, and cost-effective in comparison with paper-based payment systems.**

**What is an Electronic Payment System?**

**Electronic Payment System allows people to make online payments for their purchases of goods and services without the physical transfer of cash and cheques, irrespective of time and location. The key components of this payment system are the payers and payees, financial institutions, electronic devices, communication networks, payment gateways, and mobile payment apps. As the global economy continues to evolve, the dependency on physical modes of payment is gradually giving way to digital alternatives that offer speed, convenience, and efficiency. These systems facilitate a diverse range of financial activities, from online purchases and bill payments to person-to-person transfers.**

#### Types of Electronic Payment System

**India, being the fastest-growing economy and a developing nation, has witnessed significant growth in various types of Electronic Payment Systems, driven by technological advancements and efforts to promote a cashless economy. The prominent types of Electronic Payment Systems in India range from the Unified Payments Interface (UPI) to Debit and Credit cards. Listed below are the types of Electronic Payment Systems:**

1. **Unified Payments Interface (UPI):**

[**UPI**](https://www.npci.org.in/what-we-do/upi/product-overview) **has become a widely adopted and popular electronic payment system in India. It enables users to link multiple bank accounts to a single mobile application, allowing seamless and instant fund transfers between individuals and merchants.**

1. **Mobile Wallets:**

**Mobile Wallet services like Paytm, PhonePe, and Google Pay have gained widespread acceptance. Users can load money into these digital wallets and use the balance for various transactions, including mobile recharge, bill payments, and online shopping.**

1. **Debit and Credit Cards:**

**Debit and Credit card usage is prevalent in India, with various banks issuing these cards for electronic transactions. Cards are commonly used for Point-of-Sale (POS) transactions, online purchases, and cash withdrawals from ATMs.**

1. **Immediate Payment Service (IMPS):**

**IMPS enables instant interbank electronic fund transfers through mobile phones, internet banking, or ATMs. It is particularly useful for peer-to-peer transactions and small-value payments.**

1. **National Electronic Funds Transfer (NEFT):**

**NEFT is a nationwide electronic payment system that facilitates one-to-one funds transfer between bank accounts. It operates on a deferred settlement basis and is widely used for both individual and corporate transactions.**

1. **Real-Time Gross Settlement (RTGS):**

**RTGS is another electronic fund transfer system that allows real-time settlement of largevalue transactions. It is typically used for high-value interbank transfers.**

1. **Prepaid Instruments:**

**Prepaid Instruments, including prepaid cards and gift cards, provide users with a convenient way to make electronic payments with a pre-loaded amount.**

### Advantages of Electronic Payment System

* **24/7 Accessibility: Electronic Payments can be made at any time, providing round-theclock access to financial transactions.**
* **Global Accessibility: Users can make payments and transfer funds globally without being restricted by geographical boundaries.**
* **Instant Transactions: Electronic Payments are processed quickly, allowing for nearinstantaneous transfer of funds between accounts.**
* **Faster Settlement: Compared to traditional payment methods, electronic transactions often result in faster settlement times.**
* **Record-Keeping and Tracking: Electronic Payment Systems facilitate easy recordkeeping for both businesses and individuals.**
* **Encryption and Authentication: Electronic Payment Systems employ robust encryption and authentication protocols to secure transactions and protect sensitive information.**

### Disadvantages of Electronic Payment System

* **Security Concerns: Electronic Payment Systems are susceptible to security breaches, including hacking, phishing, and identity theft.**
* **Technical Issues: Electronic Payment Systems rely on technology, and technical glitches or system failures can disrupt transactions.**
* **Fraud Risk: Despite security measures, Electronic Payment Systems are not immune to fraud. Unauthorized transactions, stolen credentials, or fraudulent activities can occur, leading to financial losses for individuals and businesses.**
* **Privacy Concerns: Users may be concerned about the collection and storage of personal information by electronic payment providers.**
* **Transaction Fees: Some electronic payment systems impose transaction fees, which can add up over time.**

### Regulatory Bodies Governing Electronic Payment System in India

* **The Regulatory Framework for the Electronic Payment System in India is governed by the Reserve Bank of India and other relevant authorities. The Reserve Bank of India has the authority to oversee and regulate payment and settlement systems.**
* **The** [**Payment and Settlement Systems Act, 2007**](https://www.rbi.org.in/commonperson/english/scripts/FAQs.aspx?Id=420) **provides the legal framework for the regulation and supervision of payment systems in India.**
* **The** [**National Payments Corporation of India (NPCI)**](https://www.npci.org.in/) **issues guidelines for the UPI. The** [**Information Technology Act, 2000,**](https://www.meity.gov.in/content/information-technology-act-2000-0) **provides a legal framework for electronic transactions and addresses issues related to electronic governance.**
* **The** [**Securities and Exchange Board of India (SEBI)**](https://www.sebi.gov.in/) **regulates securities and capital markets, and it also regulates electronic payments where security transactions are involved.**
* **The** [**Ministry of Finance, t**](https://financialservices.gov.in/beta/en)**hrough its various departments, provides overarching policy direction and guidance related to the financial sector, including Electronic Payment Systems.**
* **The** [**Department of Telecommunication**](https://dot.gov.in/) **oversees the Telecommunications sector, and its regulations impact mobile-based electronic payment services. Mobile network operators and telecom service providers are subject to the regulations set by the DoT.**
* **The** [**Insurance Regulatory and Development Authority of India (IRDAI)**](https://irdai.gov.in/) **regulates the insurance sector in Ind**

# E-cash

**E-cash is a paperless cash system which facilitates the transfer of funds anonymously. E-cash is free to the user while the sellers have paid a fee for this. The e-cash fund can be either stored on a card itself or in an account which is associated with the card. The most common examples of e-cash system are transit card, PayPal, GooglePay, Paytm, etc.**

**E-cash has four major components-**

1. **Issuers - They can be banks or a non-bank institution.**
2. **Customers - They are the users who spend the e-cash.**
3. **Merchants or Traders - They are the vendors who receive e-cash. 4. Regulators - They are related to authorities or state tax agencies.**

# Credit/Debit Cards

**Debit Cards and Credit Cards are two of the most commonly used financial tools as far as personal finance is concerned. Despite their similarities in appearance and usage, they function quite differently. Understanding the difference between Debit Card and Credit Card is crucial for managing your finances effectively.**

**This post looks into the key distinctions, advantages and potential drawbacks of both, helping you make informed decisions about which card to use in various situations.**

**What is a Debit Card?**

**A** [**Debit Card**](https://www.icicibank.com/personal-banking/cards/debit-card) **is linked directly to your bank account and allows you to spend money you already have. When you use a Debit Card for a purchase, the amount is deducted immediately from your bank account. Debit Cards are typically issued by your bank or credit union when you open a Checking or Savings Account.**

## Key features of Debit Cards

1. **Immediate Deduction: Funds are instantly withdrawn from your bank account at the point of sale.**
2. **No Interest Charges: Since you are using your own money, there are no interest charges on transactions.**
3. **ATM Access: Debit Cards can be used to withdraw cash from ATMs.**
4. **Spending Limit: Your spending limit is the amount in your bank account.**

## Advantages of Debit Cards

**Banks offer many perks and benefits with a Debit Card**

1. **Budget friendly: Helps manage your budget, as you can only spend what you have.**
2. **Ease of Use: Convenient for everyday transactions and ATM withdrawals.**

## Disadvantages of Debit Cards

**Although there are multiple advantages of using a Debit Card, there are certain points to be cautious about. Here are a few things you need to keep in mind:**

1. **Limited Fraud Protection: Fraud protection for Debit Cards is generally less robust than Credit Cards.**
2. **Overdraft Fees: If you spend more than your account balance, you may incur overdraft fees.**
3. **No Credit Building: Using a Debit Card does not help build your credit history or improve your credit score.**

**What is a Credit Card?**

**A** [**Credit Card**](https://www.icicibank.com/personal-banking/cards/credit-card) **allows you to borrow money from the card issuer up to a certain limit to make purchases. You need to pay the borrowed amount, typically with interest, if you do not pay the full balance by the due date. Key features of Credit Cards**

1. **Credit Limit: A maximum amount you can borrow, determined by the card issuer based on your creditworthiness.**
2. **Interest Charges: Interest is charged on the due amount if not paid in full by the due date.**
3. **Credit Score Impact: Responsible use can help build and improve your credit score, while misuse can damage it.**
4. **Rewards and Benefits: Many Credit Cards offer rewards such as cashback, travel points and other perks.**

## Advantages of Credit Cards

1. **Fraud Protection: Stronger consumer protection against fraud and unauthorised transactions.**
2. **Credit Building: This helps build your credit history and will improve your credit score if used responsibly.**
3. **Rewards: Earn rewards such as cashback, travel points and discounts.**
4. **Emergency Funds: Provides a source of funds in emergencies when you may not have cash.**

## Disadvantages of Credit Cards

1. **Interest Charges: High interest rates can lead to significant debt if balances are not paid on time.**
2. **Overspending Risk: The ability to borrow can lead to overspending and financial mismanagement.**

**Impact on Credit Score: Late payments and high balances can negatively affect your credit score.**

## Debit Card vs. Credit Card - A Comparison

**Debit Cards and Credit Cards are useful financial tools. However, one may choose either, depending on the requirements. Here are the key differences between credit card and debit cards:**

## 1. Source of Funds

* **Debit Card: Uses money directly from your bank account.**
* **Credit Card: Borrows amount from the card issuer up to a predetermined limit.**

## 2. Spending Limit

* **Debit Card: Limited to the available balance in your bank account.**
* **Credit Card: Limited to the credit limit set by the card issuer.**

## 3.Interest and Fees

* **Debit Card: No interest charges on non-EMI purchases, but potential overdraft fees.**
* **Credit Card: Interest charges if the due amount is not paid on time and potential late payment charges applicable.**

## 4. Impact on Credit Score

* **Debit Card: This does not affect your credit score.**
* **Credit Card: This can help build or damage your credit score based on usage.**

## 5. Rewards and Benefits

* **Debit Card: There are many offers on online purchases, shopping and dining.**
* **Credit Card: Offers rewards, travel points, cashback and other perks.**

## 6. Fraud Protection

* **Debit Card: Limited fraud protection may take longer to resolve disputes.**
* **Credit Card: Enhanced fraud protection through quicker resolution and less liability for unauthorised transactions.**

## When to use a Debit Card

**The Debit Card is used extensively in our day-to-day activities.**

1. **ATM Withdrawals: It is used to withdraw cash from ATMs.**
2. **Avoiding Debt: This helps to avoid the accumulation of debt as you are using your own money.**

## When to use a Credit Card

**Credit Cards are mostly used when a larger fund is required.**

1. **Large Purchases: Useful for expensive purchases that you may want to pay off over time.**
2. **Building Credit: This helps in building your credit history and improving your credit score.**
3. **Earning Rewards: Take advantage of rewards such as cashback, travel points and other benefits.**
4. **Emergency Funds: Provides a financial cushion in emergencies.**

# Digital Signature

**A digital signature is a mathematical technique which validates the authenticity and integrity of a message, software or digital documents. It allows us to verify the author name, date and time of signatures, and authenticate the message contents. The digital signature offers far more inherent security and intended to solve the problem of tampering and impersonation (Intentionally copy another person's characteristics) in digital communications.**

**The computer-based business information authentication interrelates both technology and the law. It also calls for cooperation between the people of different professional backgrounds and areas of expertise. The digital signatures are different from other electronic signatures not only in terms of process and result, but also it makes digital signatures more serviceable for legal purposes. Some electronic signatures that legally recognizable as signatures may not be secure as digital signatures and may lead to uncertainty and disputes.**

**Application of Digital Signature**

**The important reason to implement digital signature to communication is: A. Authentication**

1. **Non-repudiation**
2. **Integrity**

## Authentication

**Authentication is a process which verifies the identity of a user who wants to access the system. In the digital signature, authentication helps to authenticate the sources of messages.**

## Non-repudiation

**Non-repudiation means assurance of something that cannot be denied. It ensures that someone to a contract or communication cannot later deny the authenticity of their signature on a document or in a file or the sending of a message that they originated.**

## Integrity

**Integrity ensures that the message is real, accurate and safeguards from unauthorized user modification during the transmission.**

# Cryptography

**Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce.**

**Modern cryptography techniques include algorithms and ciphers that enable the** [**encryption**](https://www.fortinet.com/resources/cyberglossary/encryption) **and decryption of information, such as 128-bit and 256-bit encryption keys. Modern** [**ciphers,**](https://www.fortiguard.com/psirt/FG-IR-19-007) **such as the Advanced Encryption Standard (AES), are considered virtually unbreakable.**

## Public Key Cryptography

**PKC stands for Public Key Cryptography. It is also known as asymmetric cryptography. It is an encryption technique or a framework that uses a pair of keys (public and private key) for secure data communication.**

**These keys are related, but not identical keys. Each key performs a unique function, i.e., the public key is used to encrypt, and the private key is used to decrypt. The sender uses the recipient's public key to encrypt a message, and the recipient uses the private key to decrypt this message. The use of two keys enables PKC to solve challenges faced in other cryptographic techniques.**

**PKC is different from the symmetric key algorithm, which uses only one key to both encrypt and decrypt. The two types of PKC algorithms are RSA (Rivest, Shamir, and Adelman) and Digital Signature Algorithm (DSA). PKC encryption evolved to meet the growing need for secure communication in multiple sectors such as the military, government offices, etc. This type of cryptography has become an important element of modern computer security and a critical component of the cryptocurrency system.**

**How Does PKC Work?**

**The public key is used by the sender to encrypt information, whereas the private key is used by a recipient to decrypt it. The public key can be shared without compromising the security of the private one. All asymmetric key pairs are unique, so a message encrypted with a public key can only be read by the person who has the corresponding private key.**

**The keys of a pair are mathematically related, and their length is much longer than those used in symmetric cryptography. So, it is not easy to decipher the private key from its pubic counterpart. RSA is one of the most common algorithms for asymmetric encryption in use today.**

**Benefits of PKC: o One key cannot be derived from another key, and there is no need to exchange the keys**

* **It allows to establish authentication of the sender by using PKC (digital signature) o It can be used to create a digital signature in the Operating System software such as Ubuntu, Red Hat Linux packages distribution, etc.**

**Applications of Public Key Cryptography: o Emails can be encrypted using public-key cryptography to keep their content confidential**

* **Secure socket layer (SSL) protocol also uses asymmetric cryptography to make secure connections to websites**
* **It is also used in blockchain and cryptography technology. For example, while setting up a new cryptocurrency wallet, a pair of keys is generated.**