

Data Base Management System

Introduction

Data हरुलाई जुनसुकै समयमा हेर्न, खोज्न, प्रयोग गर्न र परिवर्तन गर्न बनाइएको data हरुको संगठित समुहलाई database भनिन्छ| Telephone diary, student attendance sheet, dictionary book आदि database का उद्धारण हरु हुन्|

Database Management System

Data वा databaseलाई जुनसुकै समयमा हेर्न, खोज्न, प्रयोग गर्न र परिवर्तन गर्ने प्रयोग गरिने software packageलाई Database Management System भनिन्छ| MySQL, Oracle, Fox pro, MS-Access आदि database management system का उद्धारण हरु हुन्|

Advantages:

- केंद्रिकित प्रणालीमा data भण्डार हुने भएकाले data दोहोरिने समस्या कम हुन्छ|
- Data को गोपनियता, अखण्डता र उपलब्धतालाई सुनिश्चित गर्न मद्दत गर्दछ|
- Data हेर्ने, खोज्ने, प्रयोग गर्ने र परिवर्तन गर्ने समय न्यूनीकरण गर्न मद्दत गर्दछ|
- Data हरु सङ्कल, व्यवस्थापन र भण्डार गर्न मद्दत गर्दछ|
- Data लाई भविष्यमा प्रयोग गर्न वा क्षति भएमा पुन प्राप्त गर्ने backup को रूपमा data हरु भण्डार गर्दछ ।
- Authenticity, encryption, access control आदि विशेषता भएकाले data हरु लाई cyber attack र fraud हरु बाट सुरक्षित राख्न मद्दत गर्दछ|
- बहुप्रयोगकर्ता प्रणालीमा विकास भएकाले विभिन्नस्थान बाट आवश्यकता अनुसार data प्रयोग गर्न सकिन्छ ।

Disadvantages

- प्रारम्भिक चरणमा hardware, software र networking पुर्बधारको आवश्यकता परे हुदाँ, यसलाई कार्यन्वयन गर्न खर्चिलो हुन्छ|

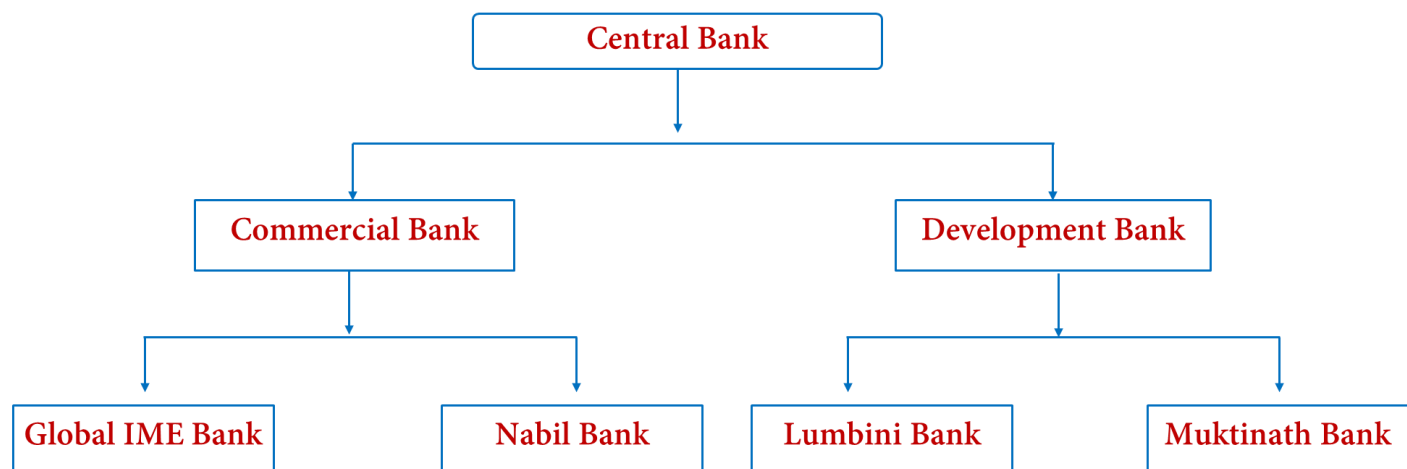
- Networking प्रणाली मा संचलान हुने हुदाँ, data हरु cyber attack र fraud बाट असुरक्षीत हुन्छन्|
- निरन्तर रुपमा data समाबेस गर्दा databaseको आकार ठुलो हुन् गई क्षति हुने सम्भावना हुन्छ|
- यसलाई सन्चालन गर्न का लागि प्राविधिक जनसक्तिको आवश्यकता पर्दछ|
- केन्द्रिकित प्रणालीमा data सङ्कलन हुने हुदाँ data हरु दोहोरिने र चुहावट हुने सम्भावना हुन् सक्दछ|
- सन्चालन गर्न धेरै memory space र कम्प्युटरको कार्य क्षमता उच्च हुनु पर्दछ|

Types

Database types/model

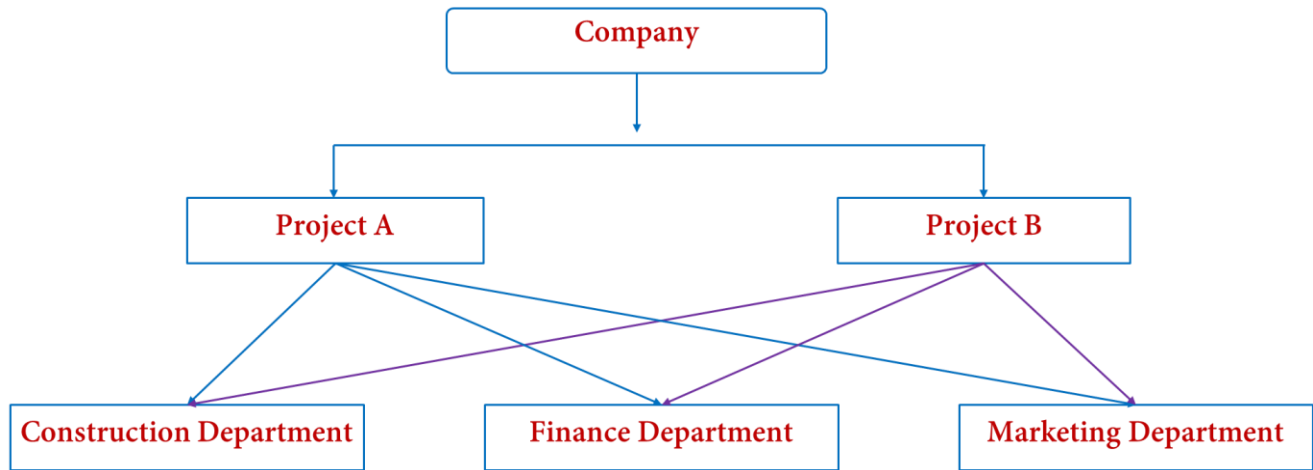
क. Hierarchical Database Model

- श्रेणीबद्ध रुपमा डाटाहरुलाई one to many relationship कायम गरि व्यवस्थापन गर्न प्रयोग गरिने database model लाई Hierarchical Database Model भनिन्छ|



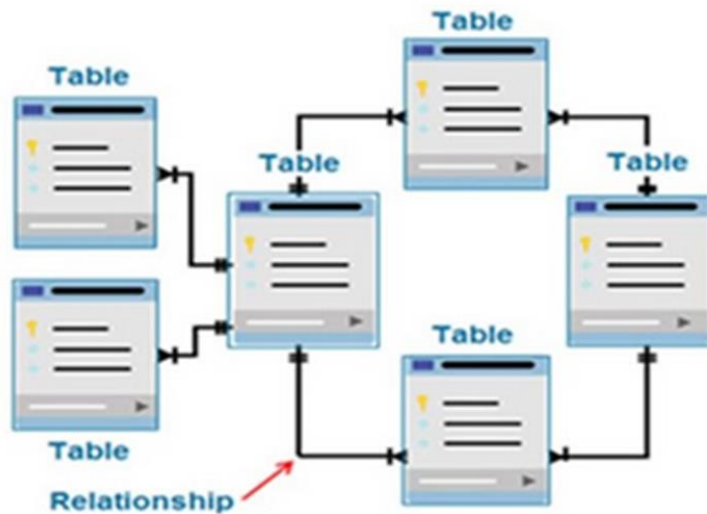
ख. Network Database Model

- श्रेणीबद्ध रुपमा डाटाहरुलाई many to many relationship कायम गरि व्यवस्थापन गर्न प्रयोग गरिने database model लाई Network Database Model भनिन्छ|



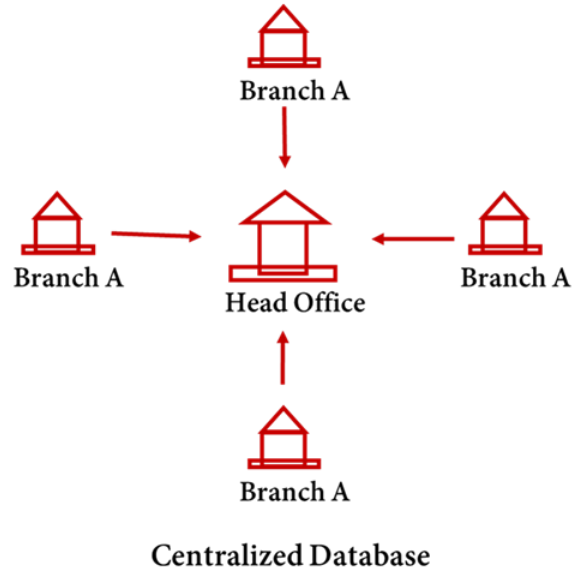
ग. Relational Database Model

- डाटाहरूलाई Row र Column को आधारमा table हरु बिच सम्बन्ध बनाई क्रमबद्ध रुपमा मिलाएर राख्न प्रयोग गरिने database model लाई Relational Database Model भनिन्छ ।



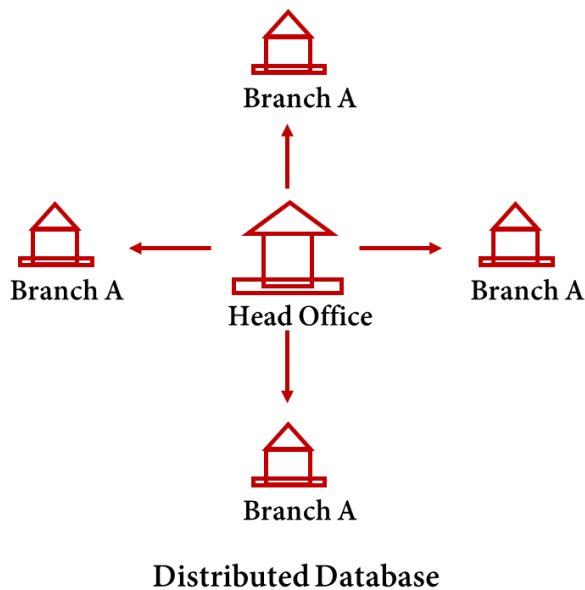
घ. Centralized Database Model

- विभिन्न शाखा वा स्थानमा भएका data हरु संकलन गरि केंद्रिकित प्रणालीमा व्यवस्थापन गर्न प्रयोग गरिने database model लाई Centralized Database Model भनिन्छ ।



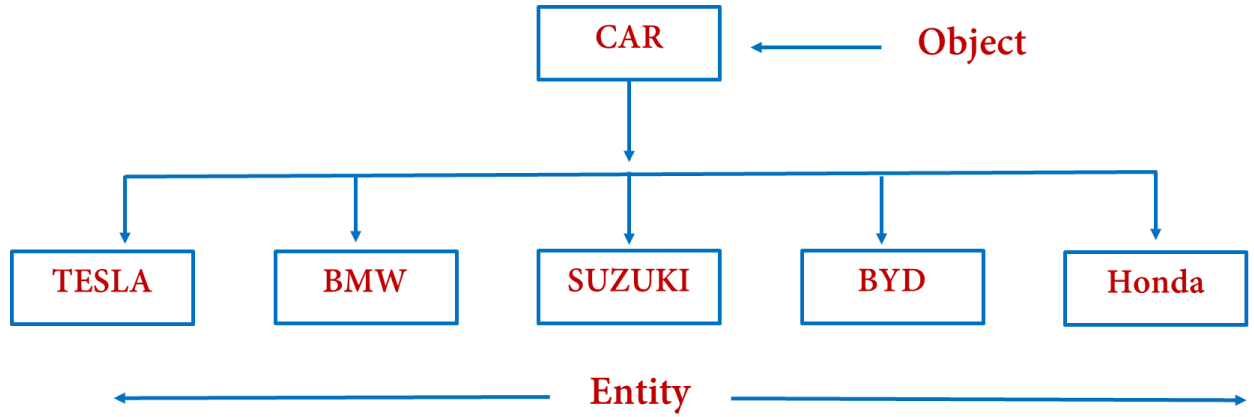
ड. Distributed database model

- केन्द्रमा भएका dataलाई विभिन्न शाखामा उपलब्ध गराउनकालाई प्रयोग गरिने database model लाई Distributed database model भनिन्छ ।



Object oriented database model (OODM)

- निश्चित object को विभिन्न entity बनाई data हरु वक्स्थापन गर्न प्रयोग गरिने database model लाई Object oriented database model भनिन्छ| C++, Java जस्ता Object oriented programming language मा OODM प्रयोग गरिन्छ|



Computer Threats and Security

Computer Threats

- कम्प्युटर प्रणालीमा भएका data, program, hardware साथै अन्य networking स्रोतहरूलाई अनाधिकृत रूपमा प्रयोग गर्ने र क्षती पुर्याउने तत्वहरूलाई कम्प्युटर threats भनिन्छ|
- Types
 - Physical Threats
 - Non Physical Threats
- a. Physical Threats:

कम्प्युटर प्रणालीमा जडान गरिएका hardware, networking उपकरणजस्ता सम्पूर्ण भौतिक साथै यान्त्रिक पाट पुर्जाहरूलाई क्षती पुर्याउने threats लाई physical threats भनिन्छ। प्राकृतिक तथा मानवनिर्मित प्रकोप, भौतिक चोरी हरु physical threats का उद्धारणहरु हुन्।

b. Non-Physical Threats:

कम्प्युटरमा भएका data, program र application हरुलाई अनधिकृतरूपमा प्रयोग गर्ने र क्षती पुर्याउने threats लाई non physical threats भनिन्छ। Malicious program जस्तै virus, worms, spyware, phishing, ransomwares, adware, trojan आदि non physical threats हुन्।

I. Virus:

- Website साथै विभिन्न applicationको माध्यम द्वार कम्प्युटर मा स्वचालित रुपमा भण्डार भइ कम्प्युटर मा भएका data, programलाई क्षति पुर्याउने malicious program लाई virus भनिन्छ।
- Virus ले कम्प्युटरको कार्य प्रणाली सुस्त बनाउन र software हरुलाई संचालन हुन् अबरोध पुर्याउन महत्वपूर्ण भुमिका खेल्छ।
- File infecting virus, macro virus, boot sector virus, multipartite, resident आदि कम्प्युटर virusका उद्धारण हुन्।

II. Phishing

- Credit Card, Login password, transaction pin आदि अनाधिकृत रुपमा प्रयोग गरि प्रयोगकर्ता गोप्य data चोरी गर्ने malicious program लाई phishing भनिन्छ। अनाधिकृत website, spam email आदि को पहुच बाट phishing हरु कम्प्युटर मा आउने गर्दछन्।

III. Spyware

- Website वा अन्य networking स्रोत हरु बाट कम्प्युटर मा स्वचालितरूपमा आएर प्रयोगकर्ताको data अनधिकृत रुपमा सङ्कलन गरि अन्य अनधिकृत व्यक्तिलाई पठाउने malicious program लाई spyware भनिन्छ।

- File download वा application install गर्दा spyware हरू कम्प्युटरमा स्वचालितरूपमा आउने गर्दछन्|

IV. Adware

- Websiteका स्रोतहरु हेर्ने वा खोल्ने कर्ममा बिज्ञापन देखाई प्रयोगकर्ताको data चोरी गरि आफ्नो अनकुल प्रयोग गर्ने malicious program लाई adware भनिन्छ|

V. Trojan

अनाधिकृत रुपमा कम्प्युटर प्रणालीलाई नियन्त्रण गरि प्रयोगकर्ताको data वा networking स्रोत हरुलाई क्षती पुर्याउने र स्वचालित रुपमा कम्प्युटरमा replicate हुने malicious program लाई Trojan भनिन्छ|

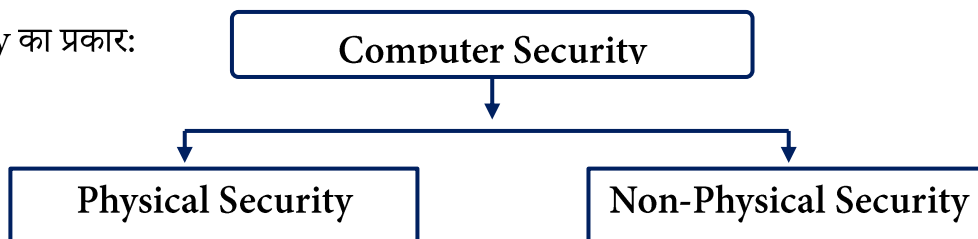
VI. Ransomware

प्रयोगकर्ताको कम्प्युटरमा भएका data हरू अनाधिकृतरूपमा encrypt (पढ्न नसकिने रुपमा) गरि प्रयोगकर्ता ले नबुझे रुपमा रुपान्तरण गर्ने र प्रयोगकर्तालाई प्रयोग गर्ने का लाई पैसामाग्ने malicious program लाई Ransomware भनिन्छ|

Computer Security

कम्प्युटरमा भएका data, program साथै अन्य networking स्रोतहरुलाई अनाधिकृत पहुँच, प्रकोप साथै virus, spyware, adware, worms जस्ता malicious program बाट सुरक्षित राख्ने प्रक्रियालाई कम्प्युटर security भनिन्छ|

कम्प्युटर security का प्रकार:



a. Physical Security:

- छुन र देख्न सकिने Computer प्रणाली मा भएका hardware, networking जस्ता भौतिक साथै यान्त्रिक पाट पुर्जा हरुलाई अनाधिकृत पहुँच साथै भौतिक वा प्राकृतिक प्रकोपबाट सुरक्षित राख्ने security लाई physical security भनिन्छ।
- Regular maintenance, free from dust, consistent power supply, appropriate temperature, regular technical support, strong and well managed lab room आदि physical securityका उद्धारण हुन्।

b. Non Physical Security

- कम्प्युटरमा भएका data, program वा अन्य networking स्रोत हरुलाई अनाधिकृत पहुँच, malicious program भौतिक वा प्राकृतिक प्रकोपबाट सुरक्षित राख्ने security लाई Non Physical Security भनिन्छ।
- Data security, network security, application security आदि Non Physical Security हरु हुन्।

Data security:

- कम्प्युटरमा भएका data हरुलाई अनाधिकृत पहुँच, प्रकोप साथै virus, spyware, adware, worms जस्ता malicious program बाट सुरक्षित राख्ने प्रक्रियालाई data security भनिन्छ।
- Firewall, authentication, data encryption, data backup आदि data security का उद्धारण हुन्।

Application security:

- कम्प्युटरमा भएका software वा program हरुलाई malicious program बाट सुरक्षित राख्ने र softwareमा आएका coding त्रुटी हरुलाई समाधान गर्ने security लाई application security भनिन्छ।
- Software update, installing antivirus software आदि application security का उद्धारण हुन्।

Network Security:

- Network, server, वा data center हरुलाई अनधिकृत पहुँच र malicious program बाट सुरक्षित राख्ने securityलाई network security भनिन्छ|
- Firewall, authentication, data backup, data encryption आदि network security का उद्धारण हुन्|

Security Mechanism:

- DataEncryption
- Firewall
- Multiple factor Authentication
- Data backup and recovery
- Data erasure
- End User Education

a. Multifactor Authentication:

- आधिकारिक प्रयोगकर्तालाई प्रमाणिकरण गर्ने प्रक्रियालाई authentication भनिन्छ।
- अनाधिकृत पहुँच बाट सुरक्षित हुन का लागि विभिन्न password तथा pin code प्रयोग गरि आधिकारिक प्रयोगकर्तालाई प्रमाणिकरण गर्ने प्रक्रियालाई Multifactor Authentication भनिन्छ।

b. Data Erasure:

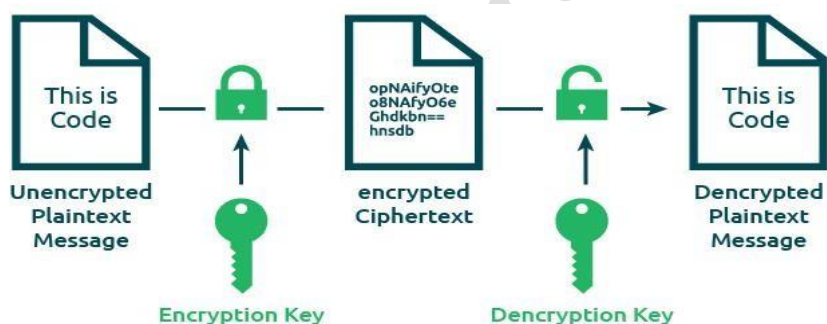
- Disk वा Drive हरु मा हुने अनावश्यक साथै निस्कृय data हरु हटाउने प्रक्रिया लाई data erasure भनिन्छ।

c. Backup and Recovery policy

- Data लाई भविष्यमामा प्रयोग गर्न वा क्षति भएमा पुन प्राप्त गर्नका लागि server, hard drive आदिमा सुरक्षित बनाई व्यवस्थापन गर्ने अभ्यासलाई Backup and Recovery policy भनिन्छ।

d. Data Encryption:

- अनाधिकृत पहुँच बाट data सुरक्षित राख्न readable data(Plain text) लाई unreadable data (cipher text)मा रूपान्तरण गर्ने (process of converting plain text to cipher text)प्रक्रियालाई Data Encryption भनिन्छ।



e. Using Utility Software

- Antivirus, antispyware, windows defender जस्ता utility software प्रयोग गरि कम्प्युटर मा भएका data, program र अन्य कम्प्युटरका स्रोतहरूलाई virus, worms, spyware जस्ता malicious program हरु बाट सुरक्षित राख्न सकिन्छ।

f. End user education

- कर्मचारी वा ग्राहक हरुलाई साइबर ज्ञान प्रदान गरि cyber fraud र attack पहिचान गर्न र सामधान गर्न क्षमतावान बनाउने अभ्यास लाई end user education भनिन्छ।

g. Firewall:

- Private networkमा भएका data, server वा अन्य networking स्रोतहरु लाई public network को माध्यम द्वारा आउने अनाधिकृत पहुँच बाट सुरक्षित राख्न प्रयोग गरिने network security वा network traffic controller लाई firewall भनिन्छ।
- Networking प्रणालीमा कार्य सम्पादन गर्ने बैंक जस्ता संगठनहरुले आफ्नो data, सम्बेदनशील दस्तावेज साथै server हरुलाई अनाधिकृत पहुँच बाट सुरक्षित राख्न firewall प्रयोग गर्दछन्।

