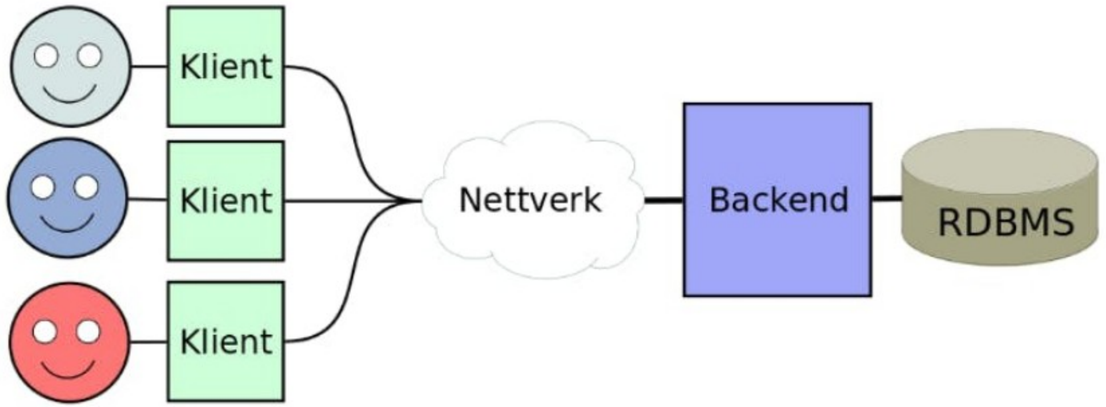
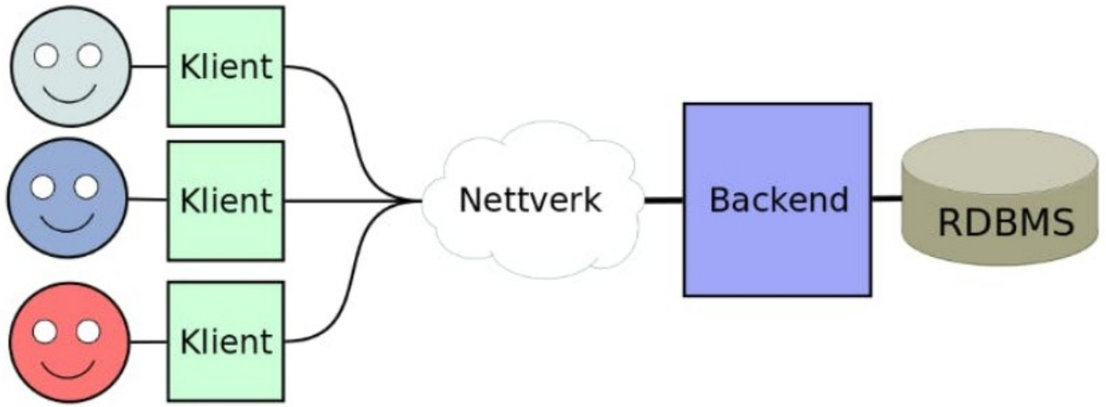
Sikkerhet, relasjonell algebra og ER

Av Katrine :)



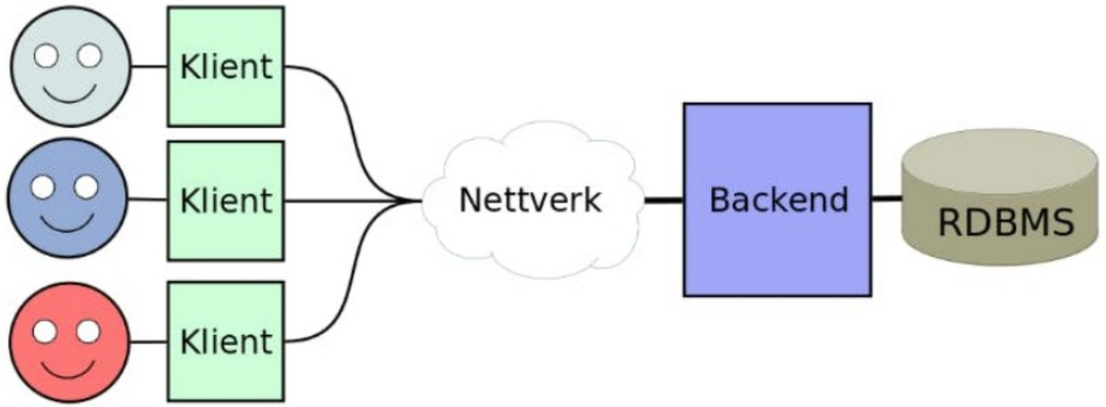
Sikkerhet

- Sikkhetsbrudd kan forekomme i alle ledd
- Klient/Frontend: autentiserer og sjekker rettigheter
- Klient/Frontend: backend og database må stole på klienten
- Klient/Frontend: trenger sikring for at bare klient har tilgang bakover
- Backend: autentiserer og sjekker rettigheter
- Backend: har ofte en bruker til databasen
- Backend: database må stole på backend
- Backend og database ligger ofte bak samme brannmur
- Database: autentiserer bruker direkte
- Database: hver bruker av programmet får hver sin databasebruker
- Database: klient kan forhåndssjekke



Tilgangskontroll

- Tilgang til databasen kontrolleres gjennom:
- Brukere
- Roller
- Rettigheter
- Roller inneholder rettigheter som mange brukertyper ofte felles har behov for
- Tenk Devilry:
- Rollen student: levere og kommentere obliger i emner knyttet til din profil
- Ikke tilgang til andres obliger
- Roller retter: se, kommentere, rette (gi godkjent/ikke godkjent) og utvide frister
- Ikke tilgang til å fjerne studenter fra kurset
- Se forelesningsfoiler for hvordan opprette og gi ut roller



Tilgangskontroll tilkoblinger

- Forrige uke snakket vi om connection objekter
- Disse kan føre til det som kalles minnelekasjer om tilkoblingen ikke avsluttes
- Derfor bør man sørge for at tilkoblingene avsluttes når man er ferdig med dem
- Tenk nettbank vs uio konto
- Lukker du siden med nettbanken, må du logge inn på nytt
- Uio konto er du logget inn på i en viss periode eller til du bytter passord
- Sikkerhet vs brukervennlighet

SQL injeksjon

- En form for angrep hvor noen kjører egen SQL kode på databasen
- Rettet mot klient/backend
- Unngår autentisering og lar folk hente, slette og endre data

SQL injeksjon

- cur.execute("SELECT username, name FROM ws.users WHERE username = %s AND password = %s;", (username, password))
- For de som har begynt med oblig 5, så har dere kanskje lagt merke til bruk av placeholders
- Om placeholders ikke blir brukt, lar det folk gjøre dette:
- SELECT * FROM products WHERE navn = 'Socks'; DROP TABLE products;
- Placeholders gjør SQL injeksjoner veldig lett å forhindre!
- Mange nettsider lagd uten det, som gjør at SQL injeksjon er på verdenstoppen av hackerangrepsmetoder
- Rettighetskontroll gjør at SQL injeksjon ikke får tilgang til data allikevel
- Viktig med sikkerhet i hvert ledd!

REPETISJON

I dag - relasjonell algebra, ER diagrammer

Neste uke - realisering, dekomponering

Basic	Derived and Auxiliary	Extended

• Selection (σ)
• Projection (π)
• Cartesian product ($\times$)
• Set operations
  • Union ($\cup$)
  • Difference ($-$ or $\setminus$)
	• Renaming (ρ)
	• Join ($\bowtie$)
	  – Theta, equi, natural, etc.
	• Set operations
	  – Intersection ($\cap$)
	  – Division ($\div$)
		• Aggregate functions and grouping (γ)
		• Generalized projection
		• Sort (τ)
		• Duplicate elimination (δ)

Relasjonsalgebra

→ Selection = WHERE

→ Projection = SELECT

→ Theta JOIN = implisitt join (WHERE clausuler)

→ Equi JOIN = inner og outer join (likhetskrav)

Skriv det som en spørring

Mentimeter

The correct answer is: select fødselsdato from Student where navn='Sara';

Skriv det som en spørring

The correct answer is: select studentNr from Student where studie='Informatikk' or studie='Matematikk';

Skriv det som en spørring

Mentimeter

The correct answer is: select * from (select * from Student where addresse='Sognsveien 1') where studie='Matematikk';

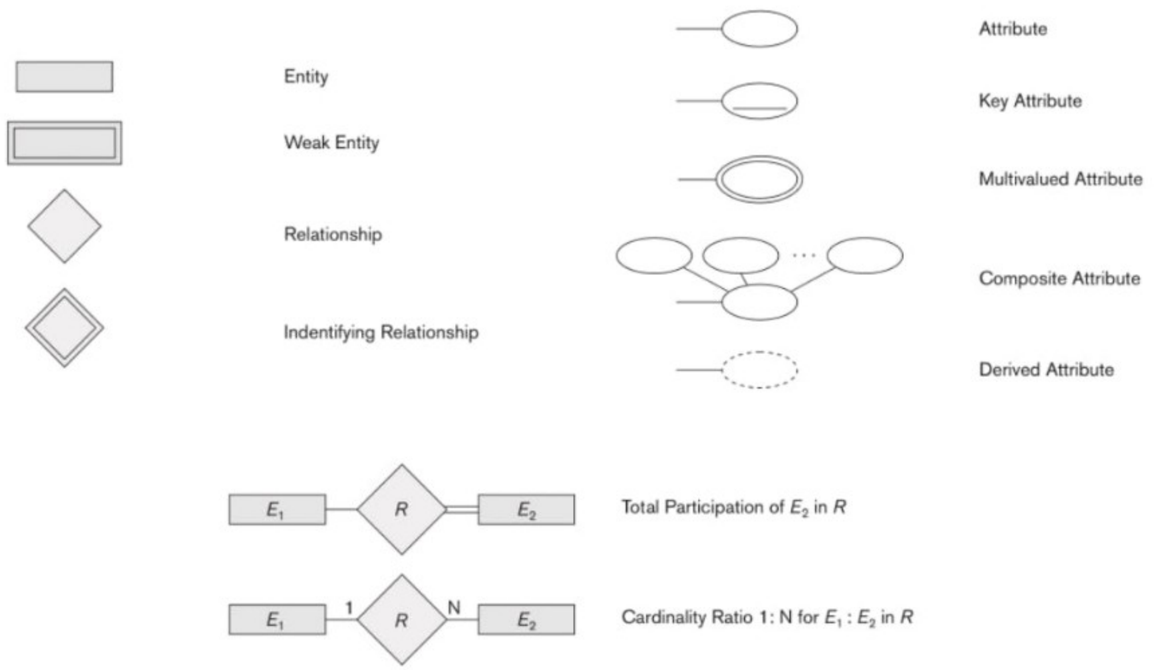
Leaderboard

Mentimeter

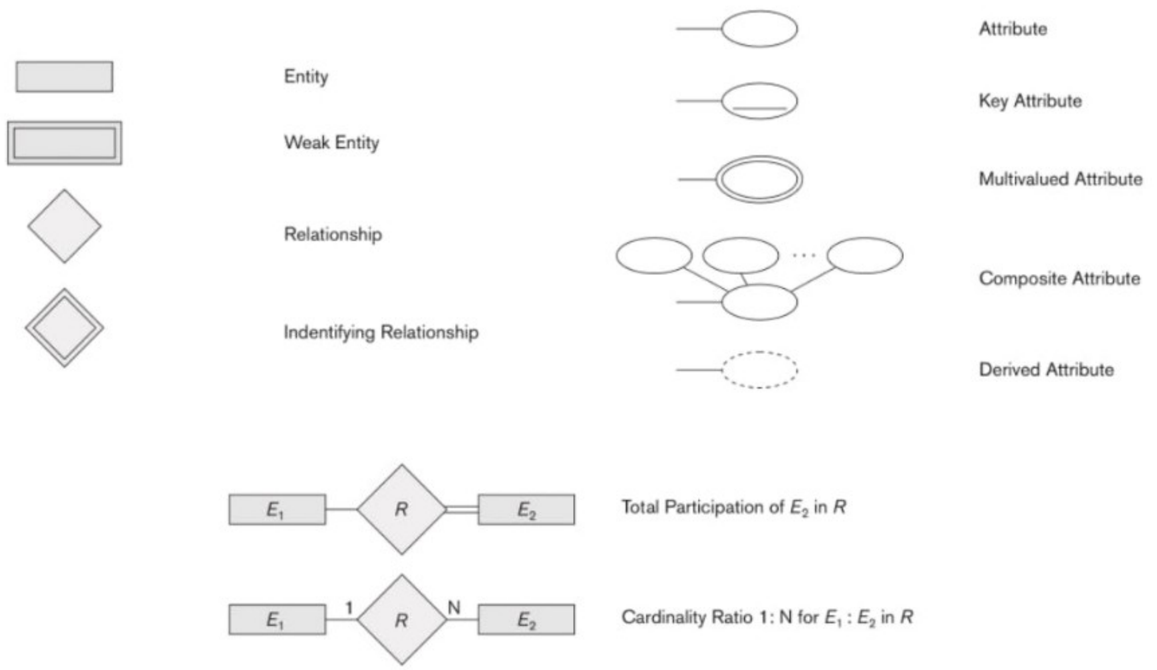
No results yet

Top Quiz participants will be displayed here once there are results!

ER diagrammer



- Entitet: Bok, Person, Land, etc
- Svak entitet: Entitet som ikke kan identifiseres på egen hånd
- Eks. Kapittel i en Bok, Kontakt til en Person, Innbygger til et Land, etc
- Forhold: Viser forholdet mellom to attributter, som Bok - Forfatter, etc
- Identifiserende forhold: Viser hvilken entitet det er som identifiserer den svake entiteten, som Land - President, etc
- Total deltakelse: Alle E2 må ha et R-forhold til E1, enhver E1 kan ha et R-forhold til E2
- Kardinalitet: Hver (1) E1 kan ha et R-forhold til ingen eller flere E2, mens flere E2 kan ha et forhold til én E1



ER diagrammer

- Attributt: Oval med attributtnavn, Navn, Fødselsdato, etc
- Nøkkelattributt: Oval med strek under attributtnavn, svak entitet har stiplet linje
- Flerverdiattributt: Dobbel oval, attributt med flere verdier, som mobilnummer, skoler, etc
- Sammensatt attributt: attributter som kan beskrives felles, som fornavn, etternavn -> navn
- Derivert attributt: Verdi vi ønsker å vise i diagrammet, men ikke lagre i tabellen, ofte heller en sprørring. Kan regnes ut med andre attributter

Hvor mange attributter har tabellen Person i databasen

Hva er riktig tolkning?

Leaderboard

Mentimeter

No results yet

Top Quiz participants will be displayed here once there are results!

THAT'S IT

:D