TECHNISCHE UNIVERSITÄT DRESDEN

PRIVACY AND SECURITY

Dresden Database Systems Group

Haupt-/Proseminar

Sicherheit in Datenbanken

Einordnung

Dresden Database Systems Group

Proseminar

- **Informatik/Medieninformatik Bachelor**: B-510, B-520, B-530, B-540, B-610
- **Informatik/Medieninformatik Diplom**: Wahlpflichtfach im Vertiefungsgebiet Datenbanken oder im Fachgebiet Architektur verteilter Systeme ab dem fünften Fachsemester
- **Wirtschaftsinformatik Bachelor**: WI-BA-08

(0 V / 2 Ü / 0 P)

Hauptseminar

- **Informatik Master**: VERT-4, INF-AQUA
- **Medieninformatik Master**: INF-AQUA
- **Informatik/Medieninformatik Diplom (2010)**: VERT-4
- **Informatik/Medieninformatik Diplom (2004)**: INF-04-HS

(0 V / 2 Ü / 0 P)

Anforderungen an DBMS

Dresden Database Systems Group

Funktionen nach Codd

1. **Integration**: einheitliche Verwaltung aller Daten
2. **Operationen**: wie Speichern, Suchen, Ändern
3. **Data Dictionary**: Datenbeschreibung der Datenbank
4. **Benutzersichten** für unterschiedliche Anwendungen
5. **Konsistenzüberwachung**: Gewährleistung der Korrektheit
6. **Datenschutz**: Ausschluss unautorisierter Zugriffe
7. **Transaktionen**: Datenbankoperationen, die als Ganzes ausgeführt werden
8. **Synchronisation** konkurrierender Transaktionen
9. **Datensicherung**: Wiederherstellung von Daten z.B. nach Systemausfällen

Anforderungen an DBMS

Dresden Database Systems Group

Funktionen nach Codd

1. Integration: einheitliche Verwaltung aller Daten
2. Operationen: wie Speichern, Suchen, Ändern
3. Data Dictionary: Datenbeschreibung der Datenbank
4. Benutzersichten für unterschiedliche Anwendungen
5. Konsistenzüberwachung: Gewährleistung der Korrektheit
6. **Datenschutz**: Ausschluss unautorisierter Zugriffe
7. Transaktionen: Datenbankoperationen, die als Ganzes ausgeführt werden
8. Synchronisation konkurrierender Transaktionen
9. Datensicherung: Wiederherstellung von Daten z.B. nach Systemausfällen

Datenschutz in DBMS

Dresden Database Systems Group

Aspekte für verschiedene Ausgangssituationen

- **Datensparsamkeit**: Die Speicherung welcher Daten ist wirklich notwendig?

	Quasi ID						
	ZIP	Age	Sex	Disease	Salary	Q1	Q2
	47677	43	Male	Heart	3.000	a1	13
	47602	22	Female	Flu	5.000	a5	4
	47678	45	Female	Hepatitis	6.000	a4	22
	47905	31	Male	HIV	4.000	a1	12
316-11-9832	Marvin	47909	36	Male	Flu	10.000	a2	8

Datenschutz in DBMS

Dresden Database Systems Group

Aspekte für verschiedene Ausgangssituationen

- Datensparsamkeit
- **Anonymisierung von Daten**: Wann und wie lässt sich bspw. bei personenbezogenen Daten eine Zuordnung vermeiden?
  - Aggregation von Daten
  - Unterscheidung zwischen verschieden sensiblen Daten

Generalization

Quasi ID			Sensitive	
ZIP	Age	Sex	Disease	Salary
47677	43	Male	Heart	3.000
47602	22	Female	Flu	5.000
47678	45	Female	Hepatitis	6.000
47905	31	Male	HIV	4.000
47909	36	Male	Flu	10.000

Quasi ID			Sensitive	
ZIP	Age	Sex	Disease	Salary
47677	40-49	Male	Heart	3.000
47602	20-29	Female	Flu	5.000
47678	40-49	Female	Hepatitis	6.000
47905	30-39	Male	HIV	4.000
47909	30-39	Male	Flu	10.000

Datenschutz in DBMS

Dresden Database Systems Group

Aspekte für verschiedene Ausgangssituationen

- Datensparsamkeit
- **Anonymisierung von Daten**: Wann und wie lässt sich bspw. bei personenbezogenen Daten eine Zuordnung vermeiden?
  - Aggregation von Daten
  - Unterscheidung zwischen verschieden sensiblen Daten

Suppression

Quasi ID			Sensitive	
ZIP	Age	Sex	Disease	Salary
47677	43	Male	Heart	3.000
47602	22	Female	Flu	5.000
47678	45	Female	Hepatitis	6.000
47905	31	Male	HIV	4.000
47909	36	Male	Flu	10.000

Quasi ID			Sensitive	
ZIP	Age	Sex	Disease	Salary
*	43	Male	Heart	3.000
47602	22	Female	Flu	5.000
47678	45	Female	Hepatitis	6.000
*	31	Male	HIV	4.000
*	36	Male	Flu	10.000

Datenschutz in DBMS

Dresden Database Systems Group

Aspekte für verschiedene Ausgangssituationen

- Datensparsamkeit
- **Anonymisierung von Daten**: Wann und wie lässt sich bspw. bei personenbezogenen Daten eine Zuordnung vermeiden?
  - Aggregation von Daten
  - Unterscheidung zwischen verschieden sensiblen Daten

Sampling

Quasi ID			Sensitive	
ZIP	Age	Sex	Disease	Salary
47677	43	Male	Heart	3.000
47602	22	Female	Flu	5.000
47678	45	Female	Hepatitis	6.000
47905	31	Male	HIV	4.000
47909	36	Male	Flu	10.000

Quasi ID			Sensitive	
ZIP	Age	Sex	Disease	Salary
~~47677~~	~~43~~	~~Male~~	~~Heart~~	~~3.000~~
47602	22	Female	Flu	5.000
47678	45	Female	Hepatitis	6.000
~~47905~~	~~31~~	~~Male~~	~~HIV~~	~~4.000~~
47909	36	Male	Flu	10.000

Datenschutz in DBMS

Dresden Database Systems Group

Aspekte für verschiedene Ausgangssituationen

- Datensparsamkeit
- **Anonymisierung von Daten**: Wann und wie lässt sich bspw. bei personenbezogenen Daten eine Zuordnung vermeiden?
  - Aggregation von Daten
  - Unterscheidung zwischen verschieden sensiblen Daten

Perturbation

Quasi ID			Sensitive	
ZIP	Age	Sex	Disease	Salary
47677	43	Male	Heart	3.000
47602	22	Female	Flu	5.000
47678	45	Female	Hepatitis	6.000
47905	31	Male	HIV	4.000
47909	36	Male	Flu	10.000

Quasi ID			Sensitive	
ZIP	Age	Sex	Disease	Salary
48689	41	Male	Heart	3.000
52288	26	Female	Flu	5.000
49985	46	Female	Hepatitis	6.000
49022	33	Male	HIV	4.000
47319	33	Male	Flu	10.000

Datenschutz in DBMS

Dresden Database Systems Group

Aspekte für verschiedene Ausgangssituationen

- Datensparsamkeit
- Anonymisierung von Daten
  - Aggregation von Daten
  - Unterscheidung zwischen verschieden sensiblen Daten
- **Vertraulichkeit:**
- Wie kann eine effiziente
- Anfrageverarbeitung
- gewährleistet werden?

```
SELECT Name, Alter
FROM Employees
WHERE Gehalt > 40000
```

Name	Alter	Gehalt	Raum
Alice	„§§$%	!&%$§§§“ %	R01
Bob	%$$%	%&/&%$§“	R01
Conny	§§$$%	$%§&!/$:§	R02
Dennis	„§$%(/	%%$§“$%/	R03

Datenschutz in DBMS

Dresden Database Systems Group

Aspekte für verschiedene Ausgangssituationen

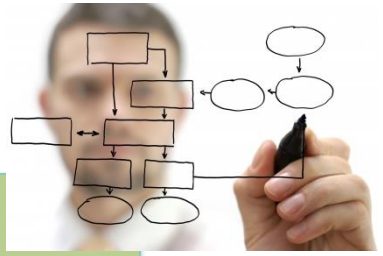
- Datensparsamkeit
- Anonymisierung von Daten
  - Aggregation von Daten
  - Unterscheidung zwischen verschieden sensiblen Daten
- Vertraulichkeit
- **Integrität**:
- Wie kann man Daten
- vor absichtlicher Verfälschung
- schützen?
  - Signaturen
  - Merkle Trees (Authenticated Datastructures)

Name	Alter	Gehalt
Alice	37	25000
Bob	55	20000
Conny	42	5000
Dennis	31	10000

Themenbereiche

Dresden Database Systems Group

Schwerpunkt: Datensicherheit in Datenbanken



Komponentenbasierte Systeme und Datenbanken

Eigenschaftserhaltende Verschlüsselungsalgorithmen

Database as a Service (DBaaS)

Sicherheitsanforderungen in Datenbanken

Ablauf

Dresden Database Systems Group

Auswahl des Themas

- Heute

Beispiel für eine Präsentation

- Obligatorisch: Teilnahme an der Belegarbeitsverteidigung am 1.11.2016

Einarbeitung in das Thema

- Bis Ende November

Ausarbeitung eines Papieres

- Bis Ende Dezember

Verteidigungsvortrag

- Januar

Regularien

Dresden Database Systems Group

Themen

- Papiere zum Thema sind auf der LV-Webseite zur Verfügung gestellt
  - Proseminar: https://wwwdb.inf.tu-dresden.de/lectures/ws-20162017/proseminar-datenbanken/
  - Hauptseminar: https://wwwdb.inf.tu-dresden.de/lectures/ws-20162017/hauptseminar-datenbanken/

Regularien

Dresden Database Systems Group

Einarbeitung in das Thema (Oktober/November)

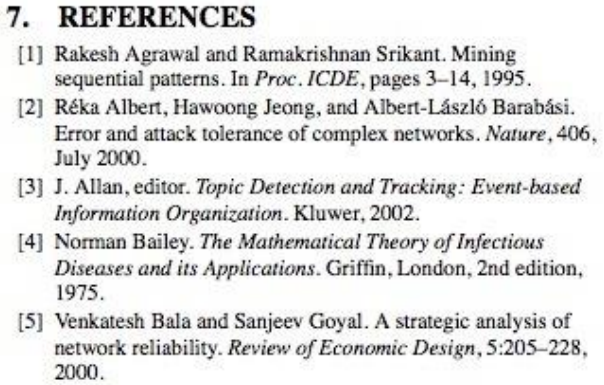
- Betreuung in Kleingruppen
- gemeinsame Treffen und Besprechungen
- Problematik verstehen und erklären können
- Betreuer
  - Beantwortet Fragen zum Thema
  - Gibt Hinweise zur Qualität der Ausarbeitung und des Vortrages

Regularien

Dresden Database Systems Group

Anforderungen

- Vorgegebene(s) Papier(e) lesen
- Darüber hinausschauen und einordnen
- Literatur Recherche (aus Uni-Netz)
  - http://dblp.uni-trier.de/
  - http://dl.acm.org/
  - http://ieeexplore.ieee.org/Xplore/dynhome.jsp?tag=1
  - http://scholar.google.de/



7. REFERENCES

[1] Rakesh Agrawal and Ramakrishnan Srikant. Mining sequential patterns. In *Proc. ICDE*, pages 3–14, 1995.

[2] Réka Albert, Hawoong Jeong, and Albert-László Barabási. Error and attack tolerance of complex networks. *Nature*, 406, July 2000.

[3] J. Allan, editor. *Topic Detection and Tracking: Event-based Information Organization*. Kluwer, 2002.

[4] Norman Bailey. *The Mathematical Theory of Infectious Diseases and its Applications*. Griffin, London, 2nd edition, 1975.

[5] Venkatesh Bala and Sanjeev Goyal. A strategic analysis of network reliability. *Review of Economic Design*, 5:205–228, 2000.

- Weitere Literatur finden
  - Keyword Suche: Sei kreativ, probiere verschiedene Schlüsselbegriffe
  - Rückwärtssuche: Welche Papiere werden referenziert?
  - Vorwärtssuche: Welche Papiere referenzieren dieses Papier?
  - Frag Deinen Betreuer ☺

How china is blocking Tor

P Winter, S Lindskog - arXiv preprint arXiv:1204.0447, 2012 - arxiv.org

Abstract: Not only the free web is victim to China's excessive censorship, but also the Tor anonymity network: the Great Firewall of China prevents thousands of potential Tor users fr... ...g the network. In this paper, we investigate how the blocking mechanism is ...

Zitiert durch: 9 Ähnliche Artikel Alle 9 Versionen In BibTeX importieren Mehr

Vorgehen - Lesen

Dresden Database Systems Group

Lesen eines Papieres - Reihenfolge

- Titel
- Abstract
- Zusammenfassung und Schlussfolgerung
- Einleitung
- Rest …

Finden guter Papiere

- Was verspricht der Titel?
- Suche Papiere zum gleichen Themengebiet.
- Unterscheide zwischen
  - Papieren, die inhaltlich einen guten neuen Beitrag leisten (großer Mehrwert) und
  - Papieren, die zwar thematisch passen, aber nur andere Annahmen treffen oder nur evaluieren (für eine Orientierung im neuen Thema kleiner Mehrwert)

Vorgehen - Lesen

Dresden Database Systems Group

Fragen an das Papier

- Auf welches Problem wird eingegangen?
- Wie ist das Problem motiviert? Warum gibt es das Problem?
- Welche Annahmen werden getroffen?
- Welche Lösung wird vorgeschlagen?
- Wie wird die Lösung evaluiert?
- Wie wird die Lösung praktisch umgesetzt?
- Was sind die Hauptbeiträge/ größten Neuerungen des Papieres?
- Bleiben Fragen unbeantwortet?
- Tauchen bei der Evaluierung oder bei den Annahmen Probleme auf?
- Ist das Papier glaubwürdig?
  - Wurde es auf einer „guten" Konferenz veröffentlicht?
  - Wurde es bereits von anderen Papieren zitiert?
  - Gibt es bereits Papiere, die Fehler in diesem Papier aufzeigen?
  - Könnte im Papier etwas vertuscht oder verschönt worden sein?

Regularien

Dresden Database Systems Group

Ausarbeitung (November)

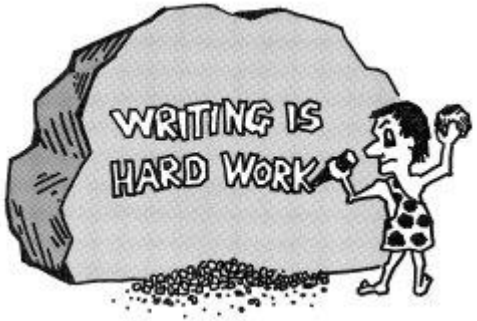
- Schriftliche Ausarbeitung des Themas in Form eines wissenschaftlichen Papieres mit angebrachter Strukturierung: Abstract, Einleitung, Literaturstand, etc.
- Vorlage: http://www.acm.org/sigs/publications/proceedings-templates
- 8-10 Seiten (Hauptseminar); 6-8 Seiten (Proseminar), deutsch oder englisch
- Abgabe: bis **2.12.2016, 24 Uhr** über das Konferenzmanagementsystem (CMS)
- Feedback kommt bis zum **9.12.2016** als Review über das CMS, auf Kritik sollte in der Ausarbeitung bzw. im Vortrag eingegangen werden
- Abgabe der finalen Version: bis **16.12.2016, 24 Uhr** über das CMS

Vorgehen - Schreiben

Dresden Database Systems Group

Gliederung eines Papieres

- Titel
- Abstract
- Einleitung
- Literatur
- Eigenanteil bzw. eigentliche Materie
  - Theorie
  - Spezifikation
  - Implementierung/Evaluation
- *Literatur alternativ hier*
- Zusammenfassung/ Zukünftige Arbeiten/Schlussfolgerung

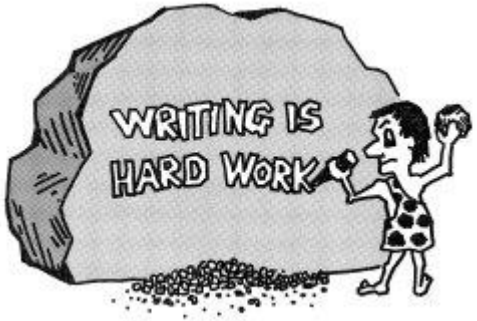


Vorgehen - Schreiben

Dresden Database Systems Group

Abstract

- **Problemaussage**
- **Relevanz**: Warum ist das Problem tatsächlich ein Problem?
- **Antwort**: Welche Lösung wird vorgeschlagen?
- **Vertrauenswürdigkeit**: Warum ist die vorgeschlagene Lösung wirklich gut?



Vorgehen - Schreiben

Dresden Database Systems Group

Einleitung

- Allgemeine Thematik, evtl. Problematik/Hintergrund allgemein erläutern für das Problemverständnis des Lesers
- Konkretes Thema, konkreter Hintergrund
- Generelles Ziel, Forschungsfragen, Motivation und Relevanz
- Warum sollte sich der Leser für das Problem interessieren?
- Evtl. verwandte Arbeiten
- Beiträge („Contributions“), die das Papier leisten soll (ca. 2-4)

Vorgehen - Schreiben

Dresden Database Systems Group

Literaturübersicht – Warum?

- Um zu zeigen, dass noch Arbeit getan werden muss
  - Warum die bisherigen Arbeiten das Problem nicht gelöst haben
  - Welche die Limitierungen der bisherigen Arbeiten sind
- Um zu zeigen, dass Du Experte bist
- Um die Verbindung zu anderen Wissenschaftsgebieten aufzuzeigen

Vorgehen - Schreiben

Dresden Database Systems Group

Literaturübersicht – Warum?

- Um zu zeigen, dass noch Arbeit getan werden muss
  - Warum die bisherigen Arbeiten das Problem nicht gelöst haben
  - Welche die Limitierungen der bisherigen Arbeiten sind
- Um zu zeigen, dass Du Experte bist
- Um die Verbindung zu anderen Wissenschaftsgebieten aufzuzeigen

Literaturübersicht – Wie?

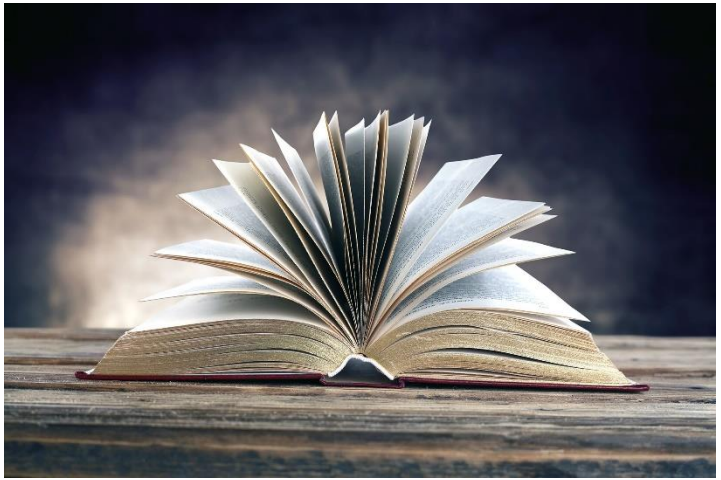
- Üblich, aber unbrauchbar: „A, B, C und D wurde getan."
- Besser: Kategorisiere und gruppiere die Arbeiten,
- begründe die Eignung in Deinem Problemkontext:
- „Lösungen A und B eignen sich für..., sind jedoch für
- ... nicht nutzbar. C und D ..."

Vorgehen - Schreiben

Dresden Database Systems Group

Literaturübersicht – Narrativ

- Erzähle eine Geschichte über das Gebiet, in dem die Literatur existiert.
- Versuche das Gebiet so zu organisieren, dass Du sehen kannst, wie sich die Arbeiten in diesem Gebiet von damals bis heute entwickelt haben.
- Ende mit Deiner Schlussfolgerung damit, dass Deine aktuelle Arbeit gebraucht wird.



Vorgehen - Schreiben

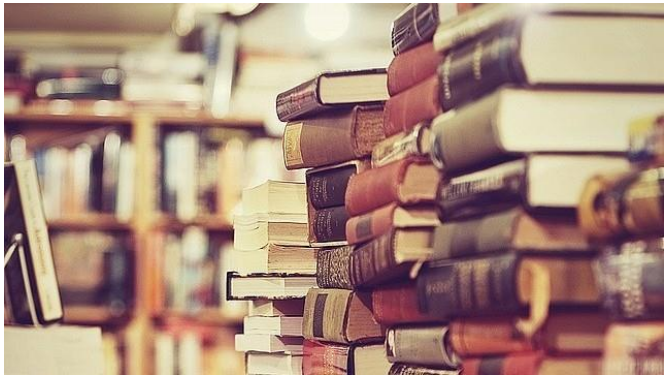
Dresden Database Systems Group

Literaturübersicht – Narrativ

- Erzähle eine Geschichte über das Gebiet, in dem die Literatur existiert.
- Versuche das Gebiet so zu organisieren, dass Du sehen kannst, wie sich die Arbeiten in diesem Gebiet von damals bis heute entwickelt haben.
- Ende mit Deiner Schlussfolgerung damit, dass Deine aktuelle Arbeit gebraucht wird.
- Beispiel:
  - (Absatz 1) Die ersten Algorithmen, A und B versuchten das Problem X zu lösen. Diese Ansätze führten mit jeweils leicht unterschiedlichen Grundannahmen zu Y und Z.
  - (Absatz 2) C, D und andere versuchten ebenfalls das gleiche Problem zu lösen, jedoch scheiterten diese Ansätze an…
  - (Absatz 3) Letztendlich waren die Autoren zu unattraktiv, um das Problem zu lösen, sodass es nun an mir hängenbleibt.

Vorgehen - Schreiben

Dresden Database Systems Group



Literaturübersicht – Zusammenfassung

- Eine gute Literaturübersicht sollte Arbeiten enthalten, die…
  - das gleiche zentrale Problem adressieren
  - verwandte Probleme adressieren
  - Dein Problem identifizieren
  - die gleichen Methoden für ein ähnliches Problem nutzen
  - Dir als Inspiration gedient haben
- Achte auf guten Schreibstil/gute Grammatik
- Überprüfe die bisherigen Arbeiten kritisch nach ihrer Relevanz und begründe
- Gehe davon aus, dass der Leser die Arbeiten und ihre Einordnung nicht kennt

Vorgehen - Schreiben

Dresden Database Systems Group

Zusammenfassung

- Fasse zusammen, was Du im Papier gesagt hast
- Was ist der Haupterkenntnisgewinn?
- Welche sind die potentiellen nächsten Schritte?

Vorgehen - Schreiben

Dresden Database Systems Group

Strukturelle Hinweise

- Sätze
  - Präsentiere Einzelaussagen: „x=y“, „Rot ist nicht blau“, „z<1 => x=y“
- Absätze
  - Aussagen, die zur gleichen Idee / zum gleichen Konzept gehören,
  - z.B. “x > 2” and “y = 7 => x > 10”
- Abschnitte
  - Kombination von Aussagen, die zum gleichen Gedankengang gehören
  - Meistens auf dem gleichen Abstraktionslevel,
  - z.B. „Grundlagen für X“, „Lösungsansätze für Y“, „neue Ideen“
- Abstraktionslevel
  - Ein Abstraktionslevel pro Absatz
  - Vom hohen zum niedrigen Abstraktionslevel oder andersherum,
  - z.B. Design -> Spezifikation -> Implementierung oder
  - Implementierung -> Spezifikation -> Design

Regularien

Dresden Database Systems Group

Vortrag

- Termine: voraussichtlich **10., 17., 24. Januar 4.DS (13.00 – 14.30 Uhr)**
- Formelle Präsentation des Themas mit Folienprojektion
- Folien deutsch oder englisch, Vortrag deutsch oder englisch
- Das Erwartungsbild entspricht dem einer Bachelor-/Belegarbeitsverteidigung
- Folien bitte 5 Tage vorher dem Betreuer zusenden, um ggf. noch Anmerkungen zu ermöglichen
- Dauer: 20 Minuten

Bewertung

- Verständnis
- Ausarbeitung
- Vortrag
- Selbständigkeit

Vorgehen - Vortrag

Dresden Database Systems Group

Strukturelle Vorschläge

- 1-2 Folien Motivation/Aufzeigen des Problems
- Lösungsansatz im Überblick
- Vorbereitung der detaillierten Erläuterung, Überblick
  - Welche Punkte möchte ich im Vortrag adressieren?
  - Wie spielen diese Punkte zusammen?
- Überblick vermitteln und „Highlights“ herausgreifen, die detaillierter erläutert werden
- Einblick in die Evaluation
  - Was wurde wie mit welchem Ziel evaluiert?
  - Was sollte gezeigt werden?
  - Was sagt die Evaluation aus?
- Zusammenfassung und Ausblick
  - Kurze Wiederholung
  - Schlussfolgerung des Papieres
  - Eigene Einschätzung/Kritik/Anwendung