

Data Science Privacy Study Guide

Josepeh Sepich Nov 7

Contents

1 Database Anonymization	4
1.1 Privacy vs Anonymity	4
1.2 EI/QI/SD	4
1.3 Challenges with protecting QI and SD	4
2 Challeneges with protecting Non-Relational Data	4
2.1 Transactional Data	4
2.2 Temporal/Longitudinal Data	4
2.3 Graph Data	4
3 K-anonymity	4
3.1 Generalization	4
3.2 Suppression	4
3.3 Equivalence Classes	4
3.4 Limitations	4
4 L-diversity	4
5 T-closeness	4
6 Attacks to K-anonymity, L-diversity, T-closeness	4
6.1 Linking Attack	4
6.2 Homogeneity Attack	4
7 Introduction to Differential Privacy	4
7.1 Definition	4
7.2 Laplace Mechanism	4
7.3 Limitations	4
7.4 Examples	4
7.5 Properties	4

8	Challeneges and Methods to address anonymity in Graph Data	4
8.1	Challeneges	4
8.2	Limitations	4
8.3	Approaches (K-degree anon)	4
8.4	De-Anonymization	4
9	Introduction to cryptography	4

1 Database Anonymization

1.1 Privacy vs Anonymity

1.2 EI/QI/SD

1.3 Challenges with protecting QI and SD

2 Challenges with protecting Non-Relational Data

2.1 Transactional Data

2.2 Temporal/Longitudinal Data

2.3 Graph Data

3 K-anonymity

3.1 Generalization

3.2 Suppression

3.3 Equivalence Classes

3.4 Limitations

4 L-diversity

5 T-closeness

6 Attacks to K-anonymity, L-diversity, T-closeness

6.1 Linking Attack

6.2 Homogeneity Attack

7 Introduction to Differential Privacy

7.1 Definition

7.2 Laplace Mechanism

7.3 Limitations

7.4 Examples

7.5 Properties

8 Challenges and Methods to address anonymity in Graph Data

8.1 Challenges

8.2 Limitations