POISONING ATTACKS
On Learned Index Structures

Evgenios Kornaropoulos
Silei Ren
Roberto Tamassia
LEARNED INDEX STRUCTURES
ML + SYSTEMS

Classic Algorithmic Approach

Key

11 30 ••• 99

1 4 5 10

11 14 21 29

110 111 113 140

In-Memory Dense Array of Sorted Keys

B-TREE
LEARNED INDEX STRUCTURES
ML + SYSTEMS

Classic Algorithmic Approach

B-TREE

In-Memory Dense Array of Sorted Keys
LEARNED INDEX STRUCTURES
ML + SYSTEMS

Classic Algorithmic Approach

New ML Approach

B-TREE

LEARNED INDEX STRUCTURE (LIS)

LEARNED INDEX STRUCTURES
ML + SYSTEMS

The case for learned index structures

Authors: Tim Kraska, Nasa Beutel, Ed H. Chi, Jeffrey Dean, Neoklis Polyzotis
Publication date: 2018/5/27
Book: Proceedings of the 2018 international conference on management of data
Pages: 486-504

Description: Indexes are models: btree-index can be seen as a model to map a key to the position of a record within a sorted array. A HashIndex as a model to map a key to a position of a record within an unsorted array and a BitmapIndex as a model to index if a data record exists or not. In this exploratory research paper, we start from this premise and posit that all existing index structures can be replaced with other types of models, including deep-learning models, which we term learned indexes. We theoretically analyze under which conditions learned indexes outperform traditional index structures and discuss the main challenges in designing learned index structures. Our initial results show that learned indexes can have significant advantages over traditional indexes. More importantly, we believe that the idea of replacing core components of a data management system through learned models has far...

Total citations: Cited by 640
ML for Systems Papers

This list is incomplete. If we are missing a paper, please email mlsyspapers@lists.csail.mit.edu and we will include it. If you would like to be informed about new research papers, subscribe here.

Acknowledgement: Parts of this list were sourced from this repository.

Table of Contents

- Tutorials / Surveys
- Learned Range Indexes
- New Learned Index Applications
- Learned Multi-Dimensional Indexing & Storage Layouts
- Learned Bloom Filters
- Hash Maps / Hashing
- Partitioning
- Data Compression
- Systems and General Optimizations
- Index Recommendation
- Configuration Tuning
- Cardinality / Selectivity Estimation
- Data-based Cardinality Estimation
- Query-based Cardinality Estimation
- Cost Estimation
- Query Optimization
- Query Processing
- Scheduling
- Caching
- Sorting
- Garbage Collection
- Sketches
- Compilation / Compilers
- SQL-Related
- Workload Related
- Data Cleaning and Exploration
ML for Systems Papers

This list is incomplete. If we are missing a paper, please email mlesyspapers@lists.csail.mit.edu and we will include it. If you would like to be informed about new research papers, subscribe here.

Acknowledgement: Parts of this list were sourced from this repository.

Table of Contents

- Tutorials / Surveys
- Learned Range Indexes
- New Learned Index Applications
- Learned Multi-Dimensional Indexing & Storage Layouts
- Learned Bloom Filters
- Hash Maps / Hashing
- Partitioning
- Data Compression
- Systems and General Optimizations
- Index Recommendation
- Configuration Tuning
- Cardinality / Selectivity Estimation
- Data-based Cardinality Estimation
- Query-based Cardinality Estimation
- Cost Estimation
- Query Optimization
- Query Processing
- Scheduling
- Caching
- Sorting
- Garbage Collection
- Sketches
- Compilation / Compilers
- SQL-Related
- Workload Related
- Data Cleaning and Exploration

285 papers
What is the Price of Learning the Patterns in the Data?
ML ATTACKS ON LEARNED INDEX STRUCTURES

New Poisoning Attacks on Cumulative Distribution Functions (CDF)

Apply Attacks on Hierarchical Learned Indexes

Test Attack on the Same Datasets + Measure Error due to Poisoning

The Price of Tailoring the Index to Your Data: Poisoning Attacks on Learned Index Structures

Ergincan E. Ekrem and Yuan Zhou

ABSTRACT

The security of learned index structures relies on the idea that the input-output functionality of such tasks can be viewed as a production task and thus, implemented using a machine learning model instead of traditional algorithmic techniques. This novel angle for a decades-old problem was inspired existing results in the protection of machine learning and data structures. However, the limitations of learned index structures, i.e., the ability to be fooled by the data they need to index, can create a situation where data poisoning becomes a viable attack vector. In this work, we present the first study of data poisoning attacks on learned index structures. Our experimental setup is different from previous works, because the dataset under poison attack is not a simple distribution function (CDF), that every instance in the training set is assigned to a single distribution. We simulated the poisoning attack on a small portion of the dataset and achieved a significant decrease in the learned index structure's accuracy. We generalize our poisoning techniques to attack the standard two-stage design of learned index structures, namely random indexes, and show that the learned index structure is vulnerable to poisoning attacks. We demonstrate the practicality of our attack and show that it is possible to design a poisoning attack that can achieve significant performance degradation in less than an hour.

CCS CONCEPTS

• Information systems → Data structures; • Security and privacy → Cryptography and other attacks; • Computing methodologies → Machine learning approaches.

KEYWORDS

Learned Index, Data Poisoning, Attack, Indexing.
New Poisoning Attacks on Cumulative Distribution Functions (CDF)

Apply Attacks on Hierarchical Learned Indexes

Test Attack on the Same Datasets + Measure Error due to Poisoning

Need to understand the worst-case behavior of learned models on data
Part-1

Attacks on (Vanilla) Regression

Part-2

Attacks on CDF Regression

Part-3

Attacks on Hierarchical Learned Index
Part-1

 Attacks on (Vanilla) Regression

 Part-2

 Attacks on CDF Regression

 Part-3

 Attacks on Hierarchical Learned Index
WHAT IS REGRESSION (VANILLA) MODEL

Regression Before Poisoning

Regression After Poisoning
WHAT IS REGRESSION
KNOWN POISONING APPROACHES

THREAT MODEL

- Attacker: Malicious contribution points
- Power: Access to data (White-box Attack)
- Goal: Degrade Performance
Poisoning point can be any \((X,Y)\)
Part-1

Attacks on (Vanilla) Regression

Part-2

Attacks on CDF Regression

Part-3

Attacks on Hierarchical Learned Index
REGRESSION IN THE CONTEXT OF LIS
WHAT’S THE DIFFERENCE?

Cumulative Density Function
REGRESSION MODEL ON CDFs
IMPACT OF AN ERROR

Prediction Error: Trigger Local Search to Fix
REGRESSION MODEL ON CDFs
POISONING CDFs

Regression Before Poisoning
Regression After Poisoning

Original Regression
Poisoned Regression
REGRESSION MODEL ON CDFs
POISONING CDFs

**Regression Before Poisoning**
- Original Regression

**Regression After Poisoning**
- Original Regression
- Poisoned Regression

Poisoning point can **NOT** be any (X,Y)
REGRESSION MODEL ON CDFs
WHAT’S THE DIFFERENCE?

Regression Before Poisoning

Regression After Poisoning

Poisoning point can NOT be any (X, Y)

is (X, rank(X))
REGRESSION MODEL ON CDFs
WHAT’S THE DIFFERENCE?

Regression Before Poisoning

Regression After Poisoning

WHAT'S THE DIFFERENCE?
**CONTRIBUTIONS**

- Give a linear poisoning attack for a **single** point
- Greedy poisoning attack for **multiple** points
- Poisoning percentage < 15%
- Evaluation Metrics:
  - Ratio Loss = Poisoned_MSE/MSE
  - Memory Offset = Predict. Location - Real Location
REGRESSION MODEL ON CDFs
EVALUATION

Uniform Key Distribution

Ratio Loss

Average Memory Offset

Poisoning Percentage

Keys: 1000 Density:5%

Keys: 5000 Density:5%

Keys: 1000 Density:10%

Keys: 5000 Density:10%

Keys: 5000 Density:50%

Keys: 5000 Density:80%

Keys: 100 Density:10%

Keys: 500 Density:10%

Keys: 5000 Density:80%

Memory Offset 125-180

200x larger MSE
Part-1

Attacks on (Vanilla) Regression

Part-2

Attacks on CDF Regression

Part-3

Attacks on Hierarchical Learned Index
ATTACK SO FAR...
ONLY REGRESSION ON CDF
HIERARCHICAL MODELS
TWO-STAGE ARCHITECTURE

Key

Model 1.1

Model 2.1

Model 2.2

Model 2.N

In-Memory Dense Array of Sorted Keys

Rank

Keys

Rank

Keys

Rank

Keys
ATTACK ON HIERARCHICAL MODELS
TWO-STAGE ARCHITECTURE

ADVERSARIAL APPROACH

- Focus on second-level poisoning (regression)
- Attacker controls
  1. how many keys per model (Volume)
  2. the location of poisoning keys per model
ATTACK ON HIERARCHICAL MODELS
TWO-STAGE ARCHITECTURE

(HIGH-LEVEL) ALGORITHM

- Distribute the **same number** of poisoning keys per model
- **Move** a poisoning key to the next/previous model if it increases the total error
- Use previous multipoint regression attack to decide which poisoning points to insert
ATTACK ON HIERARCHICAL MODELS

EVALUATION

Uniform Key Distribution

- Keys: $10^7$
- Model Size: $10^2$
- #Models: $10^5$
- Key Domain: $10^9$

- Ratio Loss

Poisoning Percentage

1% 5% 10%

α = 3
α = 2

4x larger MSE

Log-Normal Key Distribution

- Keys: $10^7$
- Model Size: $10^3$
- #Models: $10^4$
- Key Domain: $10^9$

- Ratio Loss

Poisoning Percentage

1% 5% 10%

α = 3
α = 2

150x larger MSE

3x larger MSE

30x larger MSE

300x larger MSE
The Price of Tailoring the Index to Your Data: Poisoning Attacks on Learned Index Structures

Evgenios M. Kornaropoulos
George Mason University, USA
evgenios@gmu.edu

Sidi Rez
Consul MA, USA
sidi.rez@ens.fr

Roberto Tamassia
Brown University, USA
roberto@brown.edu

ABSTRACT

The security of learned index structures relies on the idea that the input-output functionality of a classifier can be trained as a probabilistic task and thus, implemented using a mixture-of-experts learning model instead of standard approximation techniques. This yields a more accurate and more flexible classifier for a decreased learning parameter which is an important result in the presence of machine learning and data engineering. However, if the machine learning structure is not trained to deal with the lack of security, the learning model can have a serious impact on the performance of the system. In this work, we present the first study of data poisoning attacks on learned index structures. Our poisoning approach is different from additional work on the cost of index attacks to tailoring a decision distribution on DNP (DD on DNP), every instance in the poisoning of an existing index in multiple passes. We introduce the poisoning attacks on learned index structures that are applicable for both network and SQL database systems. We generate poisoning techniques to attack the two-stage design of learned index structures called Winner with Learning (WNL), which has been shown to outperform existing techniques. We evaluate our attacks under a variety of parameterizations of the model and show that the cost of the WNL increases to 4% and the size of the mounting attacks increases to 51%.

CCS CONCEPTS

- Information systems → Data structures; - Security and privacy → Cryptography and other attacks; - Computing methodologies → Machine learning approaches.

KEYWORDS

Learned Indexes, Data Poisoning, Attack Training

1 INTRODUCTION

Database systems on index structures are needed to efficiently store and access data. It is crucial to select proper software that performs well under various conditions. Efficiently engineered query optimizer is an important task in the construction of database systems. However, if the design is not properly trained with respect to the algorithm, the system design can be severely affected with a high loss risk. The work by Rovats, Biro Cita, Dova, and Pietro (2019) showed that the cost of attacks on existing index structures is a machine learning problem that the attacker can quickly use a memory location based on a hit rate-based behavior on the data at hand.

Next Steps

- First vulnerability assessment for Learned Indexes
- Introduced the “security mindset” to discover blindspots on learned systems
- Constructive dialog between Database and Security communities

Thank you!

https://encrypted.systems

evgenios@gmu.edu