Tasha Januszewicz
Cover Letter for Discussion Leader
CSE-60876

Paper: Strengthening Order Preserving Encryption with Differential Privacy

General Topic: Using differential privacy to create a more secure order preserving encryption scheme

Specific Behavior or Activity Studied: The authors develop and test a scheme that adds differential privacy to a current order preserving encryption scheme for increased security

Specific Research Questions:

- "Is it possible to leverage the properties of DP for providing a formal security guarantee for OPEs even in the face of inference attacks?"
- What is the effectiveness and accuracy of a differential privacy order preserving scheme?

Challenges:

- Differential privacy introduces error and order preserving encryption needs to preserve order. These are contradictory.
- The scheme needs to be secure in terms of differential privacy and be immune to inference attacks.

Paradigm: The authors use a combination of theory and experimental analysis to show the efficacy and accuracy of their newly constructed encryption scheme.

Problem: Order preserving encryption is, by nature, weak to frequency-analyzing ordered chosen plaintext attacks. Given its most common usage in range queries, this attack is quite feasible even for entities to execute without breaching or modifying the system in place.

Importance: Order preserving encryption is commonly used in range queries as a part of data analytics. Using this encryption, data that is sensitive can be used in analysis by third parties and can be shared for educational purposes. If an attacker is able to leverage the queries to gain additional information on the original data, that might have serious consequences both for the people whose data is involved as well as the trust that people have volunteering their data to be distributed in the future.

Claims: The authors claim that their privacy guarantee is strictly stronger than current privacy guarantees on differential privacy They also claim that their scheme fulfills these requirements, therefore making it secure. Finally, they claim that their experiments show that the scheme has high accuracy and low overhead.

State of Knowledge: Both differential privacy and order preserving encryption have formal definitions which are built on as a part of this paper. As well, the authors use the privacy guarantees that are most often associated with those methods of encryption to build their own privacy guarantee. Finally, the authors draw on currently available schemes for both types of encryption to build their own.

Evidence: The authors use deductive reasoning and proofs to prove that their privacy guarantee is stronger than currently used in the field and to prove that their scheme satisfies this requirement. They then use empirical evidence to investigate the high accuracy of their scheme. They do this by analyzing a few data sets and calculating the percentage of missed records as well as the frequency and mean estimation of the absolute and relative error.

Story Structure: The authors of this paper set out to create a scheme that connects differential privacy and order preserving encryption and explain the importance of their task. To do that, they create a basis for this connection by defining a new, strongly stronger, security guarantee that combines the classic security guarantees from differential privacy and order preserving encryption. Once they create their privacy guarantee, they create a cryptographic primitive and use that to create their scheme along with a detailed description of the implementation. They then prove that their scheme satisfies their new security guarantee. Once they do that they use experiments to show that their scheme is reasonable to use in real life.