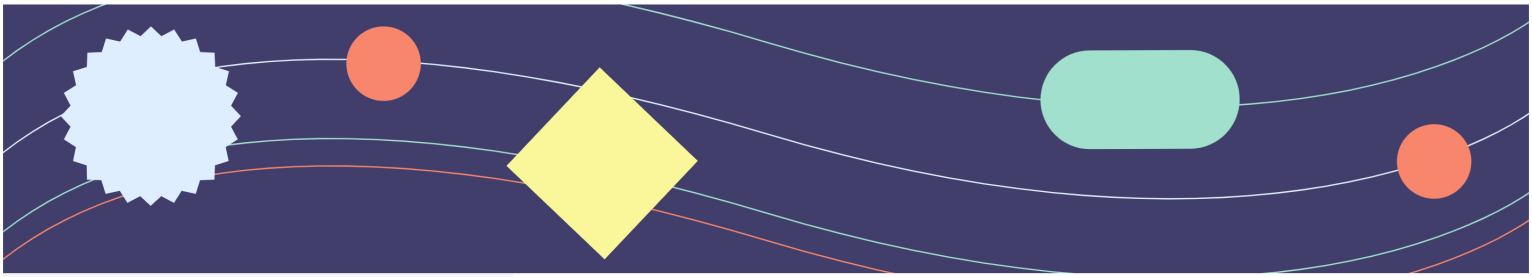

APRIL 12, 2021

Evis Drenova
Product Manager

RELATED ARTICLES

Maximize Privacy while Preserving Utility for Data Analytics

How Skyflow Helps Fintechs Comply with Financial Privacy Laws

Network Tokenization: Everything You Need to Know

Cloud Developer

Data Privacy Vault B2B B2C

Healthcare Finance

Data Security Security Vault

What is Polymorphic Encryption?

Over the last decade, businesses have significantly increased the amount of sensitive data they collect in order to create personalized customer experiences and unlock new growth opportunities. During this time, numerous high-profile data breaches have shined a light on the outdated data privacy and security practices of most businesses.

The traditional approach towards protecting sensitive data has been to use a number of encryption and tokenization solutions to de-identify the data, ensuring that it can't be exploited if it's exposed. The challenge with this approach is that once the data is encrypted, it is no longer useful to the applications and tools that need it to drive the business. This problem occurs because traditional encryption solutions don't differentiate between the types of data that they are encrypting.

A phone number is encrypted in the same way as an email address or social security number is encrypted. For decades, this has been the approach of most encryption solutions.

At Skyflow, the key insight we had is that each type of sensitive data is actually a unique data structure composed of different components which can have different use-cases. If you can identify those use-cases up front, then you can use different encryption, tokenization and redaction algorithms to run operations on fully encrypted data. We call this Polymorphic Encryption.

Polymorphic Encryption in Action

Let's look at how polymorphic encryption works on a piece of sensitive data. To start, take a phone number. If you examine a phone number closely, you'll see that it's actually a complex data type composed of three unique structures. It has a country code, an area code and a local code. Each of these components has a different use case. You might use the country code to understand how many international users it has or which call center to route an incoming call to. The area code can be used to understand customer distribution by area code or used to segment other attributes such as income by area code. Lastly, the local code may be shown in a masked form to verify the correct phone number for multi-factor authentication.

Using polymorphic encryption, we can break the phone number into its components and encrypt each one individually in order to run operations on the data without decrypting it. For example, we may encrypt the area code using an algorithm that allows us to do exact matches on fully encrypted data in order to find records in our database with the same area code. We may then use another encryption algorithm on the income field that allows us to take an average of the incomes in that area code. You can now get an idea of

the average income by area code without ever decrypting the data. Lastly, we can use a redaction algorithm on the local code to mask the first three numbers and only show the last four numbers for identity verification. This means that we've used different algorithms to facilitate different operations on fully encrypted data for different use-cases. You no longer have to trade off the utility of the data in order to keep it secure.

Performance and Scaling

By identifying the use-cases up front, we differentially encrypt the data using algorithms that allow you to run operations on the data without decrypting it.

All data coming into the platform is differentially encrypted to support many use-cases out of the box. From a performance perspective, we've architected our platform to create the different versions of the data at the time of ingestion instead of at run-time of the query. Just like traditional database systems use indexes (projections) to optimize query performance, Skyflow creates encrypted projections to optimize for query performance. This ensures that the data is optimally available in the right format significantly optimizing performance and reducing latency.

All of this functionality is available to you as a simple, clean API.

By using a single API you can retrieve different versions of the same data by simply changing a single parameter. This reduces integration and engineering complexity. You can integrate different services using the same API and retrieve different forms of the data depending on the access policies.

For example, a customer service application that should only have access to social security numbers in a redacted form can use the same API as another application that has access to social security numbers in a plain-text or masked form.

Give it a Try

Using Skyflow's polymorphic encryption engine provides you with an unprecedented level of security with a minimal impact to performance and processing speed. Most importantly, you no longer have to make the false choice between security and utility. You can use your data without compromising on security and privacy. Sign up for a demo today.