Bonafeyed's data-defined protection technology provides the means to individually secure database fields and entries rather than relying on bulk encrypting the entire database or the storage volume where it resides (aka TDE or data-at-rest, respectively). This gives database management systems, whether SQL or no-SQL based, the ability to function directly on encrypted data ensuring unauthorized accesses or breaches can only retrieve unintelligible data that cannot be exploited or monetized. The question that comes to most is how can one query and search encrypted data with results that are in human-readable form? This brief explains how SQL database queries are possible with Bonafeyed's approach. More information on how data-defined protection secures data in a database and while in-use by database backed applications, refer to "Bonafeyed Databases Protection" and "Bonafeyed Data-In-Use, respectively.

To accomplish this feat, data records are encrypted when entered or updated in a database. DBAs and the Chief Data Officers or CISOs can define the encryption schema for each data field, row, or column using a common or different 800-bit or 256-bit encryption keys. Each column can either be encrypted for order or equality preservation. Or to protect PHI and PII data fields such as social security numbers, credit card numbers or bank account information, a unique key can be used for each entry for maximum security and data obfuscation. The effect leverages millions of keys rather than just 1, yes millions, to secure the contents of a database. This means every field, column or row can be encrypted where many keys are necessary to decrypt a single record. In addition to innate data protection, this level of protection granularity permits access control to provide a legitimate multi-tenant database "row level security" implementation.

It turns out, a database does not know the difference between data that is encrypted with ***Cy4Secure*** or data that is human readable. Its only concern is that it meets the requirements of the field entry. Databases, storing Cy4Secure protected data, can still perform normal operations such as whole searches, partial searches, and groupings. When making queries, the search criteria is encrypted by ***Cy4Secure*** at the client and the database executes the query on the encrypted equivalent version of the data for exact match, starts-with, contains, ordered, or ranged. To make this possible, ***Cy4Secure*** ensures encrypted data continues to appear as data. ***Cy4Secure*** does not impose a specific encrypted data structure prior to sending other than providing the option of generating binary ASCII or hexadecimal output of the encrypted data. Otherwise, encrypted data appears as homogenized group of 1's and 0's, or unprintable characters not readily useable by an application. The data can simply be stored directly or with a tag identifying the utilized encryption key. The latter example affords a mixture of both encrypted and non-encrypted data in the same data set. A fast checksum verifies the data is encrypted and can be subsequently (after retrieving a key) decrypted prior to display or use.

In the simplest description, a search is a search. That is, any encryption operation performed during data entry can likewise be performed on any search criteria. Common grouped and cross-tabulated results can be performed on encrypted data with the added benefit of generating reports with encrypted data that is only viewable by authorized persons. Deploying Bonafeyed's ***Cy4Secure*** on database applications ensure the data fields within a database are encrypted and accessible by authorized users. In the event of a breach, the data remains secured and private from cybercriminals or in-network non-authorized users.

Contact us at info@bonafeyed.com for a demonstration or visit us at www.bonafeyed.com.