Data security using negative databases

Pramod Jagtap, CSEE, UMBC

Introduction

•Security concerns in databases.

•Current solutions: Data encryption, Query restriction, Access rights.

•Data privacy against partially-specified queries and efficient mechanism to answer fully-specified queries.

Related Work

•Determining positive information from negative databases is a NP-hard problem.

Negative Representation

•Logical complement.

•U = All possible four character strings.

DB = {emma, eric, dave}

Negative Database(NDB) = U-DB =

{aaaa, aaab, cris, john, luca, tosh,….}

There are 26^4-3 strings in U-DB.

•Positive data and Negative data :security point of view

•NDB defined over {0,1} alphabets

Database(DB)	Negative DB Before Compression	Negative DB Using * symbol
110	000	0*0
101	010	*11
001	011	100
	100	
	111	

Figure 1: Example of negative data over {0,1, *}

Proposed Architecture

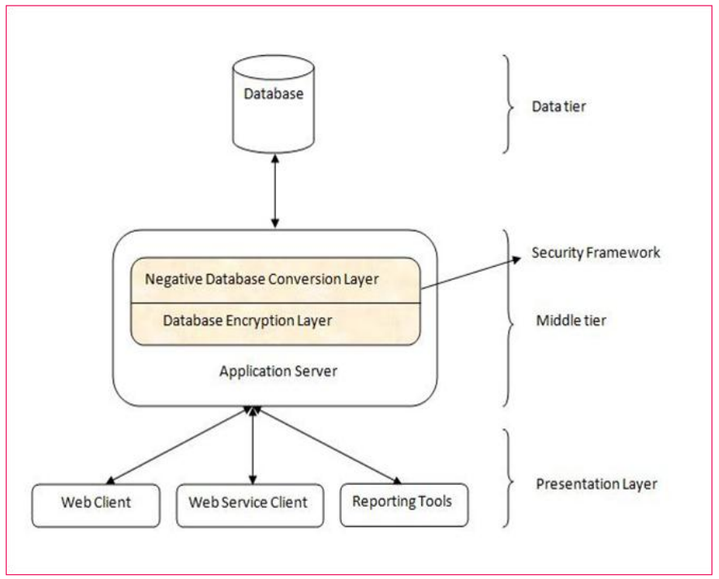

Figure 2: Proposed framework architecture

Components

•Database encryption layer : AES, variable key size .

•Negative data conversion layer : Diffusion, number of records generated depends on input field.

•Example: Customer “Alice Smith" and SSN after DE Layer is "2jNBZv“.

Customer name	SSN
Alice Smith	2c04d1
Alice Smith	j6290a
Alice Smith	Nd3416
Alice Smith	B8cc56
Alice Smith	Z063fz
Alice Smith	v3e999

Figure 3: Negative dataset for SSN field

Modified DB operations

•**Insert** : Inserts “n’ records in NDB for each record of DB.

•**Select**: Identify negative dataset and compute actual field value

•**Delete**: Delete negative dataset.

•**Update**: Identify old negative dataset, delete it and insert new negative dataset.

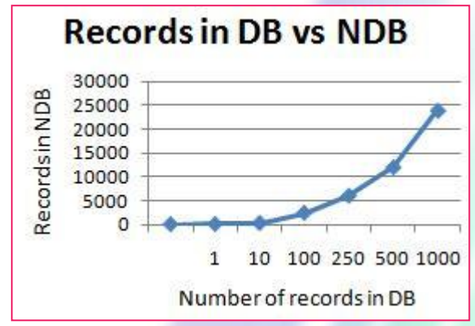

Figure 4: Records in DB vs NDB

Future work

•Performance improvement.

•Optimized way to represent negative data.

Conclusion

•Provided algorithms for storage and retrieval of negative data.

•Data privacy against partially-specified queries.

•Protect data from insider attacks

References:

•Fernando Esponda. Hiding a Needle in a Haystack Using Negative Databases, volume 5284. 2008.

•A. Patel, N. Sharma, and M. Eirinaki. Negative database for data security. Computing, Engineering and Information, 2009. ICC '09., 2:67{70, 2009.

UMBC
AN HONORS UNIVERSITY IN MARYLAND