Abstract A Trusted Cloud Database System manages client-side encrypted cloud DBs. Queries may include encryption keys. The DBS decrypts/encrypts the data on-the-fly at the cloud. Plaintext is only in protected run-time variables. Stored data are by default probabilistically encrypted through AES. Any SQL queries are feasible, with negligible processing overhead and practical storage overhead. This is a major advance over the current alternative research proposals. We detail capabilities of a trusted DBS. We adapt SQL to client-side key management. Queries may remain usually almost as non-procedural as now. A prototype implementation appears easy.

Keywords cloud DB; client-side encryption; AES; trusted DBS;
trusted

trusted

trusted

group

individual

A. Reference Architecture of a Trusted Cloud DBS
the cloud, only fugitive run-time vales, is open-ended. As
DBS research. Our requirement on sensitive data to be, at
close the trusted cloud DB content.

they contain the key(s), appear then the basic way to dis-
through malware disclosing the run-time variables while
the attacker does not learn the encryption key. Exploits
protects enough the stored data against such threat provided
est-but-curious one, an insider being most likely culprit. The
closing them. Our threat model for these is the popular hon-
the run-time values secure in practice against exploits dis-
ponent as of a vault, firewall…. Whatever the name is, it
ades. The software protection is also gradually increasing in
security of client software is a prime goal for VMs for dec-
word often. Next, the DBS should usually run in a VM. The
decade old proposals for secure VMs, [1]. Alternatively,
defense
ration for our requirement is that trusted DBSs should run

and decryption scalar functions. Our trusted cloud DBS is
current DBS could be, e.g., MySQL with its AES encryption
management we detail progressively in what follows. The

DBS with additional capabilities for client-side encryption
query processing end.

and any retrieved/calculated plaintext data, at most by the
instantiates run-time variables with the metadata brought-in.

We believe trusted DBSs a promising goal for cloud
browsers. Recall
highly volatile only. This characteristic makes them usually
DBS running on a cloud node simply as usual for software

DBS and the client. It may return selected column ciphertext
has not this capability. A smart client may send a
Fig. 1. A
circuit…, [14], [15]). One may think of the protective com-
add-on hardware (trusted computing module (TCM), FPGA

core

software (only)

smart

simple

ciphertext

moving target

defense

plaintext
B. Encryption Modes for an AES DB

**Individual deterministic encryption:**

2. Group deterministic encryption:
C. SQL for AES DBS

Trusted

Probabilistic AES DB encryption:
the default is our belief that the metadata encryption is safer

itly not to be so for specific data definition. The reason for

statement, then the key implicitly encrypts all the related

column definition. If the client provides the key in a DDL

bles. All tables share the DB key 'S-P123'. All data names

granularity.

deterministic one. The scope is according to the key

default as well. The client may override it by either type of

query.

variable only and is wiped-out once DBS processes the DDL

sons, we limit this encryption to probabilistic only. As for

knowledge of the DB evidently. For obvious practical rea-

provides elsewhere. Next, the purpose of the whole

is optional. First, the function may reuse the key that the

DBS produces the ciphertext using the AES E (X, K, E)

Create Database 'S-P' Key 'S-P123';

Create Table S S# Char (6), SNAME Varchar (40),

Create Table S pName Key 'S123', S# Char 12….

some Create Table overrides this default for itself. E.g., the

impossible. By default, all columns would be probabilisti-

P gets probabilistically encrypted for the AES DBS catalogs.

The Create Database statement has the T-SQL specific

statement.

T-SQL specific

also optional. Its absence means the default probabilistic

 encryption related alterations would do and cost similarly.

we stressed.

practice, as we stressed.

for AES DB, DBA may alter all

tables, providing then the DB key. This applies to all the

encryptions provided also through Key clause, but may result the invo-

column with its own key. The column key may be

table with its own key provided in the statement as well or

name S-P could alternatively result operationally

of, e.g., S-P name could alternatively result operationally

encryption related new features. E.g., DBA may decide to

tended similarly. Using it for AES DB, DBA may alter all

From P Key 'P123', SP, S, Key 'S-P123' Where

P.P# = SP.P# and  S.S# = SP.S# and SP.QTY > 200 ;  /* S-P

Applies by default to all columns in Select statement that is

applies by default to all columns in Select statement that is

comment, as usual after '/*'.

f o l l o w s w i t h i n t h e u s u a l V a l u e s c l a u s e .  F o r  U p d a t e s t a t e-

ment, it may follow the table name or any column modifica-

fo l l o w s w i t h i n  t h e u s u a l  V a l u e s  c l a u s e .  F o r  U p d a t e  s t a t e-

for any column with its own key. The column key may be

table with its own key provided in the statement as well or

for Select DML statement, Key clause may similarly

For the Insert DML statement, Key clause may similarly

Alter Table P Key 'S-P123' As Alter PNAME To

Alter Table DDL statement of T-SQL is supposed ex-

Alter Table P Key 'S-P123' As Alter PNAME To

Finally, Drop Table T-SQL statement is the usual

Finally, Drop Table T-SQL statement is the usual

Finally, Drop Table T-SQL statement is the usual

Finally, Drop Table T-SQL statement is the usual

Finally, Drop Table T-SQL statement is the usual

Finally, Drop Table T-SQL statement is the usual
D. T-SQL Query Execution Plans
E. Implementing AES DBS

A. Processing Overhead
B. Storage Overhead

C. Query Processing

key set-up
Insecure Persistent Cloud Storage to start practicing AES DBSs. Let us stress again that all this seems each case, a browser suffices to run plaintext queries as well.

Likewise, SQL Server seems the runner up candidate. In the homomorphic encryption, finally, AES DBS could thus be up to eighty five times faster. The queries can be also expected to be in the order of magnitude at least slower read/write speed thus. All other benchmarks we have highlighted some, see [3a] for more. The main conclusion is that it appears the first generally practical architecture for a client-side encrypted relational cloud DB. It roots in the intensive research for almost four decades. It is the only allowing for simple clients. The on-the-fly decryption/encryption by a trusted cloud processor, of 1.91 – 2.86%, [17]. With respect to processors, it is the only at present potentially offering to large public any functional probabilistic encryption. The Select SUM(x)… query adding 100K probabilistic encryption. The queries can be also expected to be in the order of magnitude at least slower read/write speed thus.

Another measure can be the AES DBS query execution time being up to eighty five times faster. The on-the-fly decryption/encryption by a trusted cloud processor, of 1.91 – 2.86%, [17]. Our scheme adding up at best 0.2ms to the AES DBS query execution environment for trusted (protected) query execution over Encrypted Cloud Databases. 8th Intl. Conf. on Data Management Systems – CHES 2015. In DEXA 2015.

Smart Client

Key(s)

p

le Client

Core plaintext DBS

Core plaintext DBS

Update

Select

Data Encryption/Decryption

Hardware AES Showdown - VIA Padlock vs Intel AES-NI vs AMD Hexacore. 2011.

http://www.grantmcwilliams.com/tech/technology/387-hardware-aes-

showdown-via-padlock-vs-intel-aes-ni-vs-amd-hexacore

https://software.intel.com/en-us/articles/intel-aes-ni-performance-

testing-on-linux-java-stack#aes256


http://www.sisoftware.co.uk/?d=qa&f=cpu_vs_gpu_crypto&l=en&a=

http://blogs.msdn.com/b/sqlsecurity/archive/2015/07/28/encrypting-


http://thinkdiff.net/mysql/encrypt-mysql-data-using-aes-techniques


http://csis.gmu.edu/albanese/events/march-2013-security-meeting/

http://thinkdiff.net/mysql/encrypt-mysql-data-using-aes-techniques

http://blogs.msdn.com/b/sqlsecurity/archive/2015/07/28/encrypting-


http://thinkdiff.net/mysql/encrypt-mysql-data-using-aes-techniques


http://csis.gmu.edu/albanese/events/march-2013-security-meeting/

thefly aes overhead of reads by SQL Server on AMD Hexacore. 2011.

Another measure can be the AES DBS query execution speed with respect to the same query over a homomorphic DBS, appears the first generally practical architecture for a client-side encrypted relational cloud DB. It roots in the intensive research for almost four decades. It is the only allowing for simple clients. The on-the-fly decryption/encryption by a trusted cloud processor, of 1.91 – 2.86%, [17]. Our scheme adding up at best 0.2ms to the AES DBS query execution environment for trusted (protected) query execution over Encrypted Cloud Databases. 8th Intl. Conf. on Data Management Systems – CHES 2015. In DEXA 2015.

Smart Client

Key(s)

p

le Client

Core plaintext DBS

Core plaintext DBS

Update

Select

Data Encryption/Decryption

Hardware AES Showdown - VIA Padlock vs Intel AES-NI vs AMD Hexacore. 2011.

http://www.grantmcwilliams.com/tech/technology/387-hardware-aes-

showdown-via-padlock-vs-intel-aes-ni-vs-amd-hexacore

https://software.intel.com/en-us/articles/intel-aes-ni-performance-

testing-on-linux-java-stack#aes256


http://www.sisoftware.co.uk/?d=qa&f=cpu_vs_gpu_crypto&l=en&a=

http://blogs.msdn.com/b/sqlsecurity/archive/2015/07/28/encrypting-


http://thinkdiff.net/mysql/encrypt-mysql-data-using-aes-techniques


http://csis.gmu.edu/albanese/events/march-2013-security-meeting/

thefly aes overhead of reads by SQL Server on AMD Hexacore. 2011.

Another measure can be the AES DBS query execution speed with respect to the same query over a homomorphic DBS, appears the first generally practical architecture for a client-side encrypted relational cloud DB. It roots in the intensive research for almost four decades. It is the only allowing for simple clients. The on-the-fly decryption/encryption by a trusted cloud processor, of 1.91 – 2.86%, [17]. Our scheme adding up at best 0.2ms to the AES DBS query execution environment for trusted (protected) query execution over Encrypted Cloud Databases. 8th Intl. Conf. on Data Management Systems – CHES 2015. In DEXA 2015.

Smart Client

Key(s)

p

le Client

Core plaintext DBS

Core plaintext DBS

Update

Select

Data Encryption/Decryption

Hardware AES Showdown - VIA Padlock vs Intel AES-NI vs AMD Hexacore. 2011.

http://www.grantmcwilliams.com/tech/technology/387-hardware-aes-

showdown-via-padlock-vs-intel-aes-ni-vs-amd-hexacore

https://software.intel.com/en-us/articles/intel-aes-ni-performance-

testing-on-linux-java-stack#aes256


http://www.sisoftware.co.uk/?d=qa&f=cpu_vs_gpu_crypto&l=en&a=

http://blogs.msdn.com/b/sqlsecurity/archive/2015/07/28/encrypting-


http://thinkdiff.net/mysql/encrypt-mysql-data-using-aes-techniques


http://csis.gmu.edu/albanese/events/march-2013-security-meeting/

thefly aes overhead of reads by SQL Server on AMD Hexacore. 2011.

Another measure can be the AES DBS query execution speed with respect to the same query over a homomorphic DBS, appears the first generally practical architecture for a client-side encrypted relational cloud DB. It roots in the intensive research for almost four decades. It is the only allowing for simple clients. The on-the-fly decryption/encryption by a trusted cloud processor, of 1.91 – 2.86%, [17]. Our scheme adding up at best 0.2ms to the AES DBS query execution environment for trusted (protected) query execution over Encrypted Cloud Databases. 8th Intl. Conf. on Data Management Systems – CHES 2015. In DEXA 2015.

Smart Client

Key(s)

p

le Client

Core plaintext DBS

Core plaintext DBS

Update

Select

Data Encryption/Decryption

Hardware AES Showdown - VIA Padlock vs Intel AES-NI vs AMD Hexacore. 2011.

http://www.grantmcwilliams.com/tech/technology/387-hardware-aes-

showdown-via-padlock-vs-intel-aes-ni-vs-amd-hexacore

https://software.intel.com/en-us/articles/intel-aes-ni-performance-

testing-on-linux-java-stack#aes256


http://www.sisoftware.co.uk/?d=qa&f=cpu_vs_gpu_crypto&l=en&a=

http://blogs.msdn.com/b/sqlsecurity/archive/2015/07/28/encrypting-


http://thinkdiff.net/mysql/encrypt-mysql-data-using-aes-techniques


http://csis.gmu.edu/albanese/events/march-2013-security-meeting/

thefly aes overhead of reads by SQL Server on AMD Hexacore. 2011.

Another measure can be the AES DBS query execution speed with respect to the same query over a homomorphic DBS, appears the first generally practical architecture for a client-side encrypted relational cloud DB. It roots in the intensive research for almost four decades. It is the only allowing for simple clients. The on-the-fly decryption/encryption by a trusted cloud processor, of 1.91 – 2.86%, [17]. Our scheme adding up at best 0.2ms to the AES DBS query execution environment for trusted (protected) query execution over Encrypted Cloud Databases. 8th Intl. Conf. on Data Management Systems – CHES 2015. In DEXA 2015.