Encryption In PostgreSQL

NTT OSS Center
Moon Insung

PGConf.ASIA 2017

Who am I

- **Moon Insung**
  - 文　仁誠（ムン　インソン）
  - 문 인성

- **Work**
  - NTT Open Source Software Center
  - PostgreSQL User Support
  - PostgreSQL Develop

- **Prev Work**
  - Developed OSS Based TV Platform (Tizen) at South Korea
    - -Developed to Broadcast System Middle ware

- **Currently Interest**
  - Security of database
  - Buffer Manager
  - OSS Community

AGENDA

- Introduction

- Database Encryption
  - 2phase encryption and Key manager

- Database Encryption
  - Transparent Data Encryption (TDE)

Introduction

Recent Data breaches Security incidents

- **currently a lot of incidents in which data breaches**
  - A Company
    - More than 3 billion user data breaches.
    - did not encrypt user data.
  - B Company
    - More than 400 million user data breaches.
    - User data was protected only by SHA-1 hashing algorithm.
  - C Company
    - More than 70 million user data breaches.
    - Unencrypted user credit card number.
  - ETC…
  - All of these security incidents occurred in 21c.

Ref : https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html
https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

Innovative R&D by NTT

Recent Data breaches Security incidents

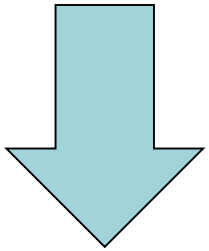
- **After data breaches security incidents, image of company?**

Credibility of the company is falling

Pay a BIG of settlement money

Recent Data breaches Security incidents

So Why were the User Data breach incidents happen?



In some cases, incidents are caused by NOT ENCRYPT DATA

Innovative R&D by NTT

Several organizations related to Data Security

Organizations and Rules to prevent of Data breaches Security incidents

PCI-DSS

HIPPA

Several organizations related to Data Security

PCI-DSS

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Ref : https://www.pcisecuritystandards.org

Innovative R&D by NTT

Several organizations related to Data Security

HIPPA

ENCRYPTING PHI

If you need to keep data and permanently deleting isn't an option, you need to encrypt PHI. This is because if an attacker is able to break into your network devices, encryption renders files useless by masking them into an unusable string of indecipherable characters.

With this danger in mind, HIPAA requires healthcare entities to "implement a method to encrypt and decrypt electronic protected health information" in requirement §164.312(a)(2)(iv). All electronic PHI that is created, stored or transmitted in systems and work devices must be encrypted (e.g., mobile phone, laptop, desktop, flash drive, hard drive, etc.).

As previously mentioned, you need to make sure that you adequately map out where PHI is created and enters your environment, what happens once PHI enters (and where it is stored), and exits your environment or organization. Although HIPAA regulations don't specify the necessary encryption, industry best practice would be to use AES-128, Triple DES, AES-256, or better.

Due to the complexity of encryption rules, healthcare organizations often use third parties to ensure encryption of PHI, partly because organizations are required to keep the tools for decryption on another device or location.

Ref : https://www.himss.org

NTT

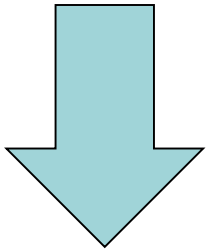
Introduction

Innovative R&D by NTT

Several organizations related to Data Security

PCI-DSS

HIPPA



Common rules include encryption of User Data

NTT

Introduction

Innovative R&D by NTT

Several organizations related to Data Security

Encrypting the user data is very important at security

NTT

Requirement for Effective Data Encryption

Rotation of encryption key should be done easily

2-Phase Encryption

Details of encryption should be hidden from application program

Transparent Data Encryption

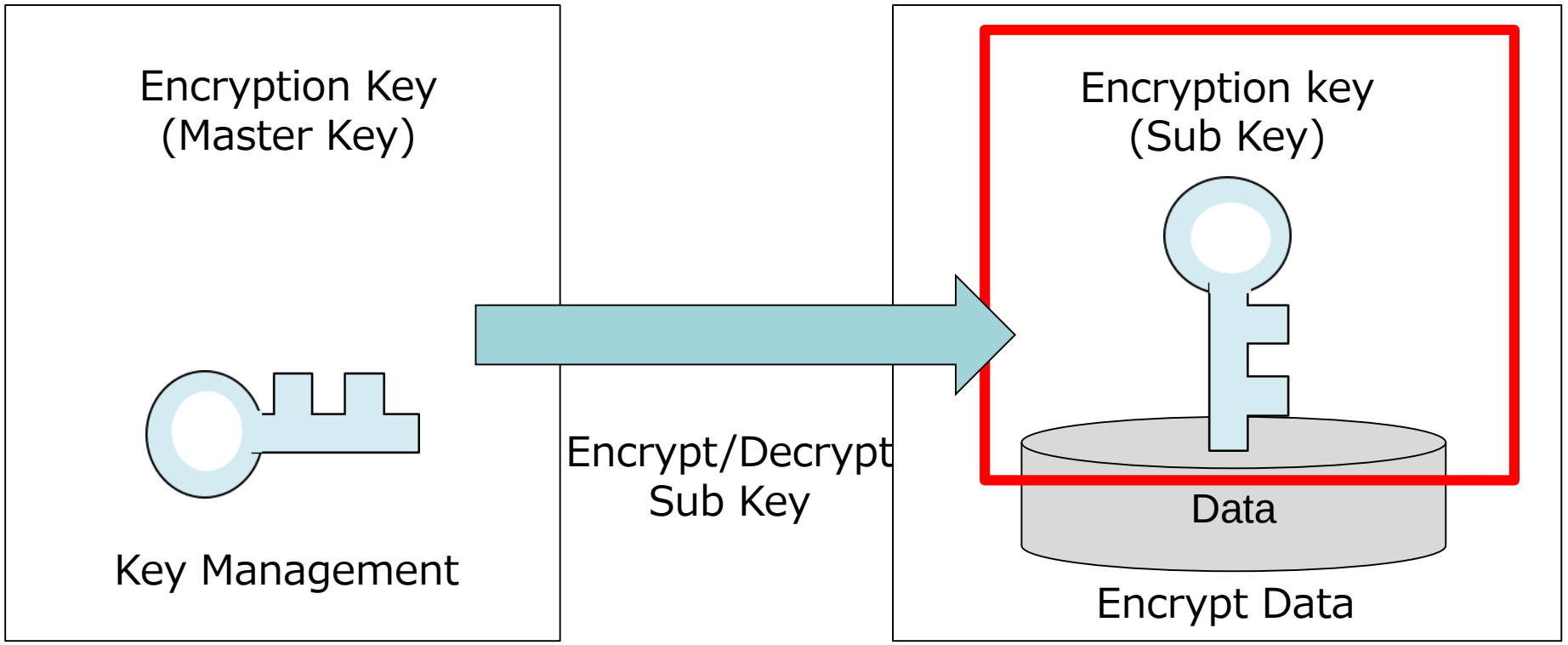
Database Encryption

2-phase encryption
Key management
At PostgreSQL

2-phase encryption

What is 2-phase encryption?

- **Two phase encryption means encrypt data and encrypt the encryption key**



2-phase encryption

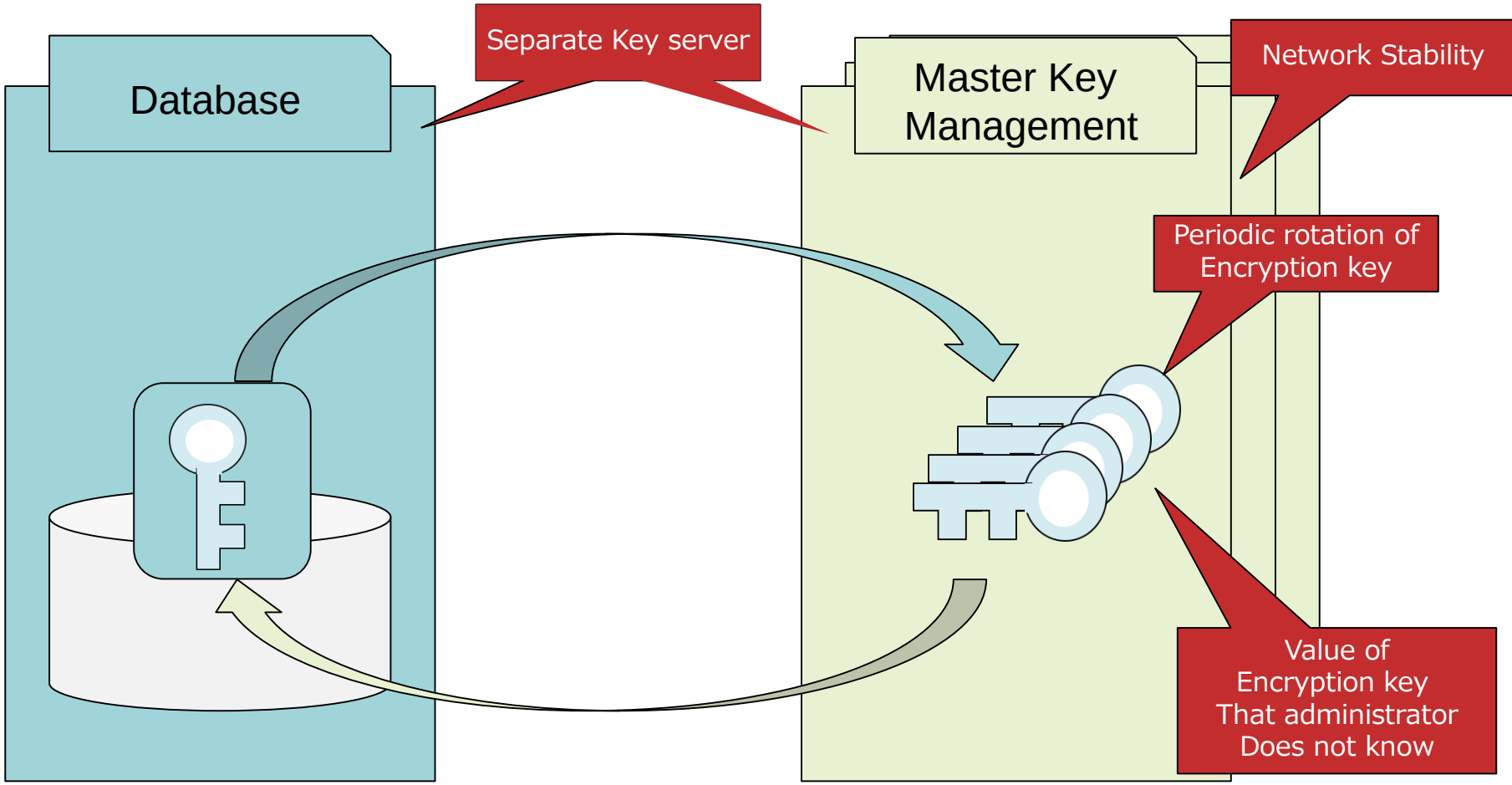
Innovative R&D by NTT

Why do need 2-phase encryption?

- More Strong Security
- Encryption Key(Master Key) rotation is convenience

2-phase encryption

What need to Implement 2-phase encryption?



2-phase encryption

Innovative R&D by NTT

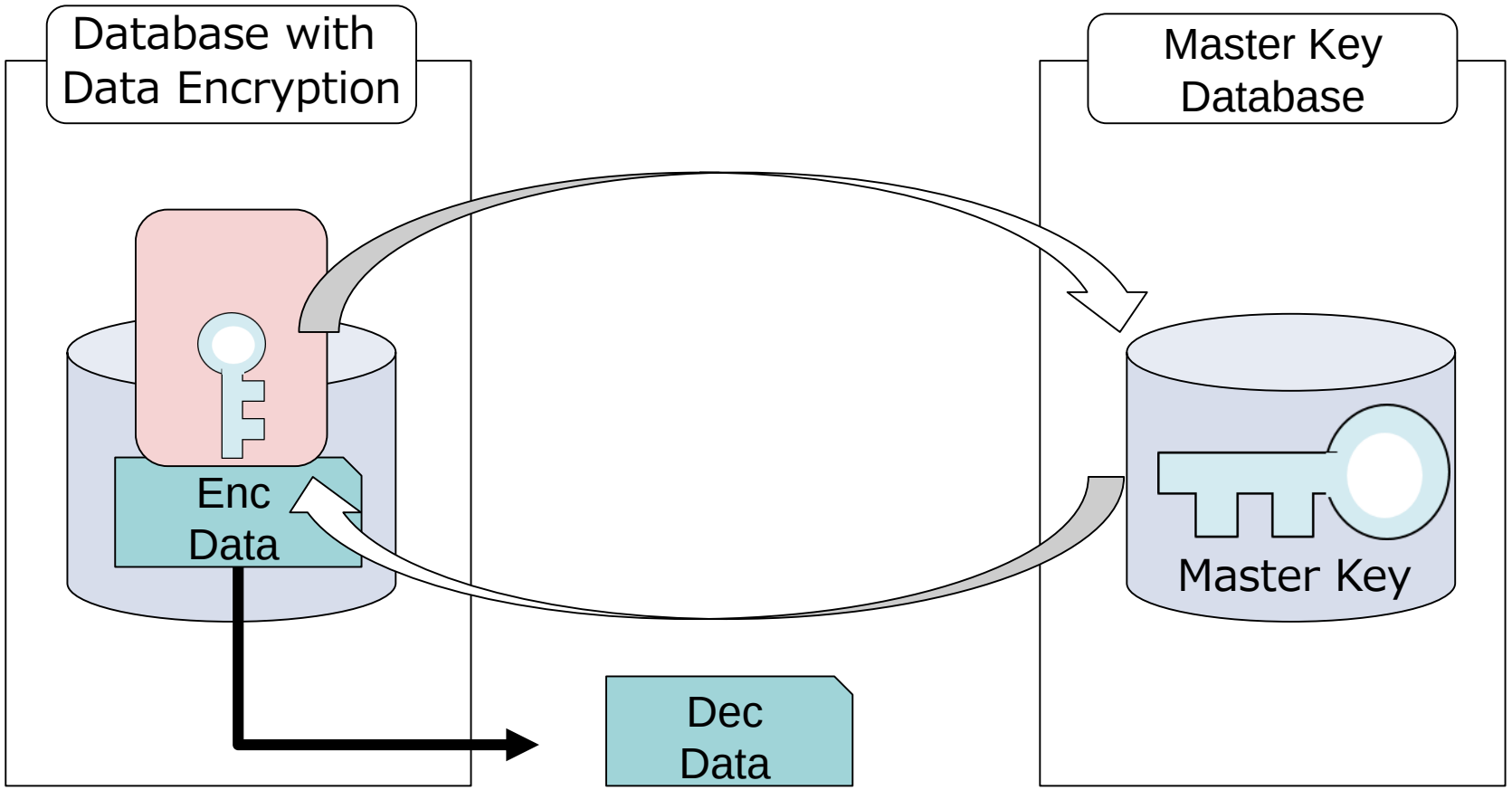
How 2-phase encryption is possible at PG?

Used Extension :
postgres_fdw, pgcrypto

NTT

2-phase encryption

How 2-phase encryption is possible at PG?



2-phase encryption

Innovative R&D by NTT

How 2-phase encryption is possible at PG?

Let’s Run Simple DEMO

NTT

2-phase encryption

Innovative R&D by NTT

Need External Tools for Strong 2-phase encryption and Key Management

- **What is Inconvenient and Difficult and lack?**
  - Server construction for Key Management is inconvenient.
  - Not officially certified Key Management and 2-Phase ENC Key
  - Value of encryption key that admin does know
  - Network Not stability

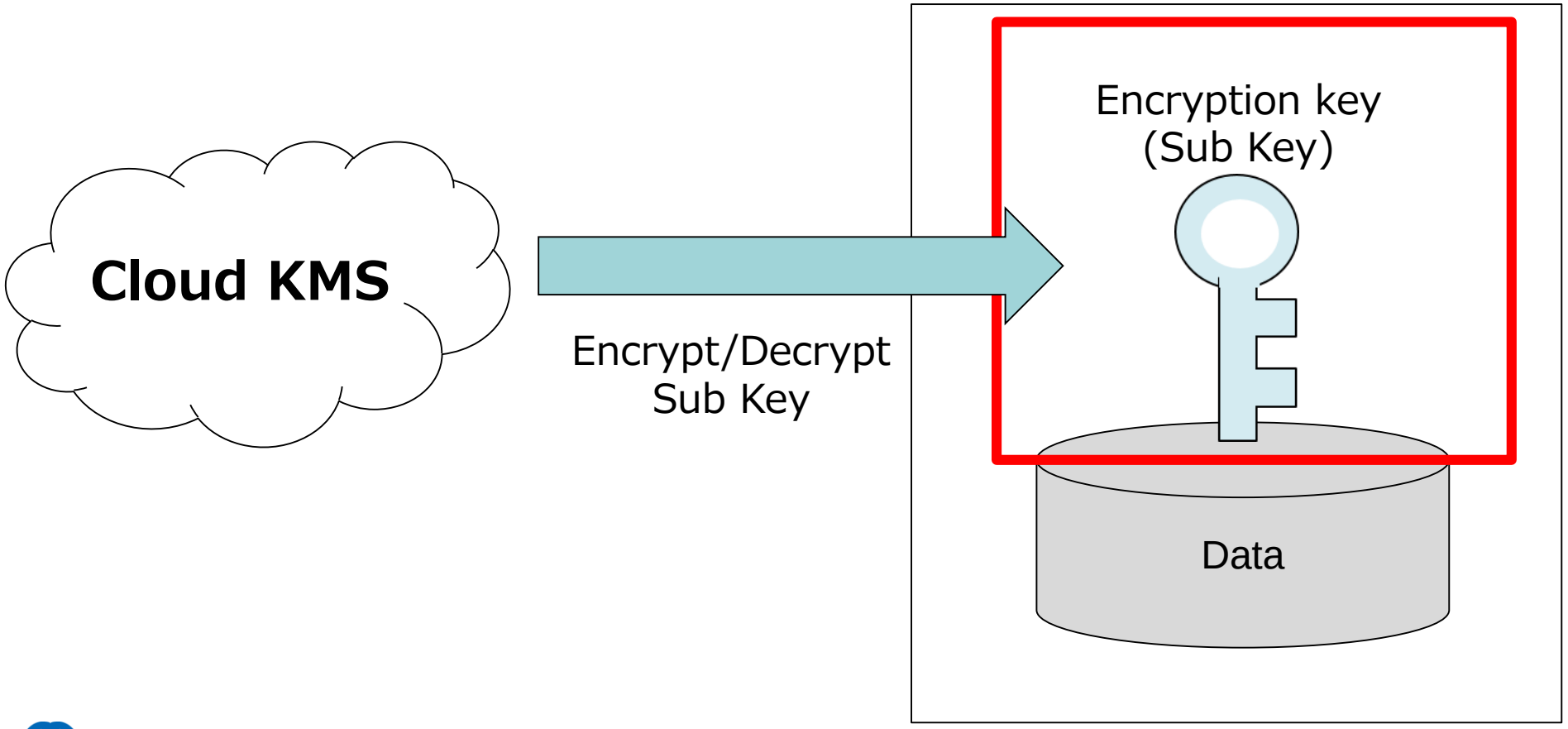
How can solve these inconveniences and difficulty and lack?

Used Hardware Security Module or Key Management Service

NTT

2-phase encryption

Need External Tools for Strong 2-phase encryption and Key Management



Innovative R&D by NTT

Roadmap of External Tools for Strong 2-phase encryption and Key Management

- **First, implement 2-phase encryption using Cloud KMS.**
  - Cloud KMS provided from “A” or “G”
    - Fees are low, widely used
  - About HSM, I just think of it now
- **I will start discussion on PG Hackers when PoC available**
- **After, other secure methods for 2-Phase Encryption will be explored**
- **If you have an interest, Please Join us!**

NTT

Database Encryption

Transparent Data Encryption At PostgreSQL

Innovative R&D by NTT

What is Transparent Data Encryption?

- **Easy to use and convenient Encryption Technology**

- **Automatically encrypt and decrypt of Data**

Innovative R&D by NTT

Why do need Transparent Data Encryption?

- **Applications and Users, do not need to know of Data Encryption**
- **Easy to migration database system encrypted with TDE**

Transparent Data Encryption

Innovative R&D by NTT

What is Transparent Data Encryption?

Ordinary Data Encryption

```
INSERT INTO encrypted_table
VALUES ( encrypt('This is Encrypted Data', 'enc_key') );

SELECT decrypt(key, 'enc_key')
FROM encrypted_table;
```

TDE

```
INSERT INTO encrypted_table
VALUES ('This is Encrypted Data');

SELECT *
FROM encrypted_table;
```

NTT

Innovative R&D by NTT

What is Transparent Data Encryption?

So is it possible to use TDE on the PostgreSQL right now?

No. Currently PostgreSQL does Not support TDE.
But, There some products can support TDE.

NTT

Transparent Data Encryption

Innovative R&D by NTT

What's are currently available TDE Products.

- **PowerGres Plus of SRA OSS, Inc.**
  - https://powergres.sraoss.co.jp/s/ja/product/PlusV94.php
- **Transparent Data Encryption for PostgreSQL of NEC Corporation**
  - http://jpn.nec.com/tdeforpg/index.html?
- **Linux dm-crypt**

NTT

Granularity of Encryption

- **Disk vs. Table level**
  - Finer grain encrypts less amount of data, needs more specified definition of data
- **Disk level encryption**
  - pros: simple definition for encryption
  - cons: all users can access encrypted data
- **Table level encryption**
  - pros: only approved user can access encrypted data
  - cons: each table should specified about encryption
- **Table level is better**
  - Cons of disk level encryption is not acceptable

Innovative R&D by NTT

Usage of Table level TDE in SQL Syntax

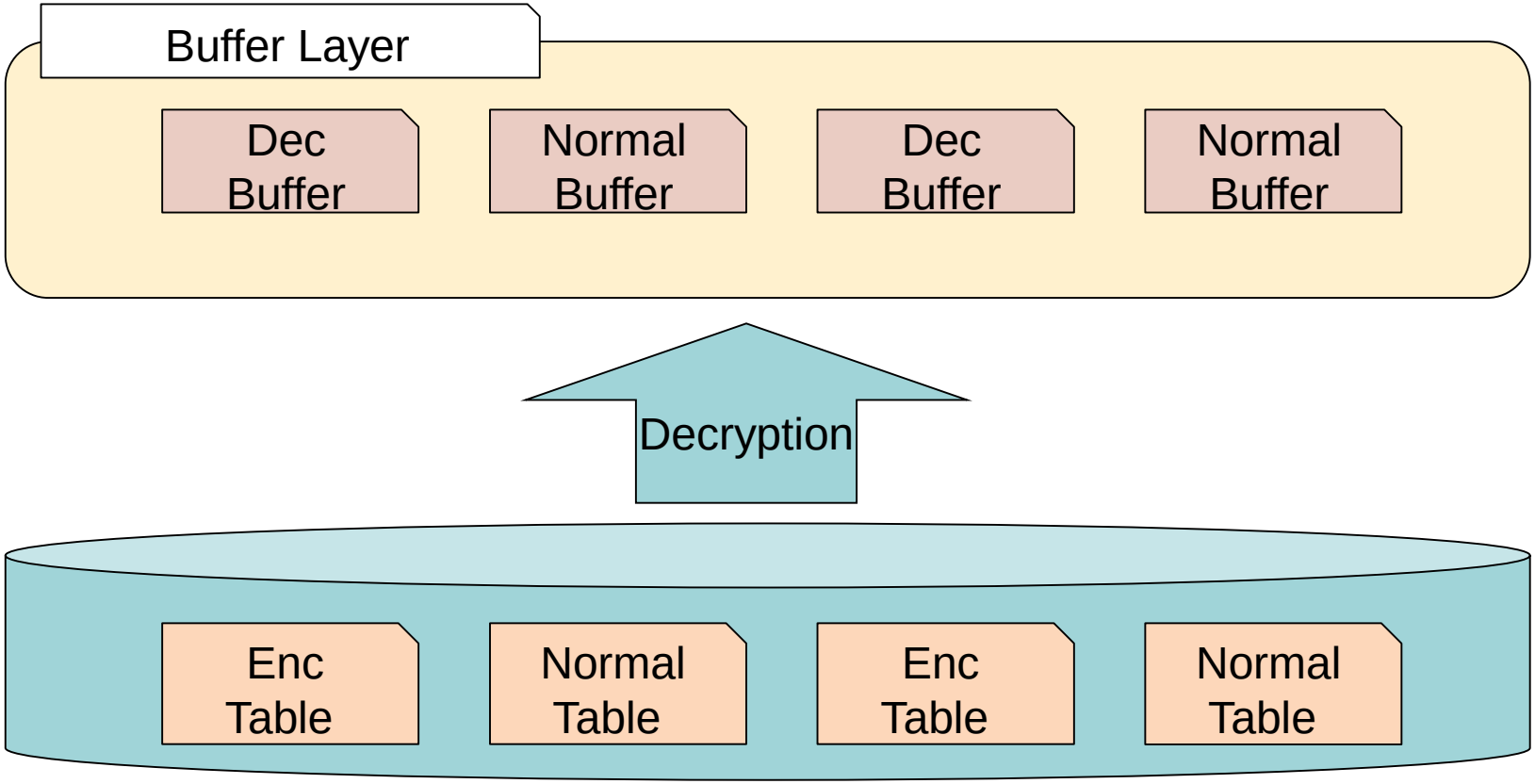
```
CREATE ENCRYPTION ON TABLE
encryption_table (contents TEXT);

INSERT INTO encryption_table
VALEUS ('What is Table Level TDE?');

SELECT *
FROM encryption_table;
```

Transparent Data Encryption

Table level TDE
Implementation with Buffer Manager



Transparent Data Encryption

Innovative R&D by NTT

DEMO

NTT

SUMMARY

SUMMARY

- **Encryption of Data is important**
  - Encryption of Data is one of the technologies to prevent User data breaches

- **Two representative technologies of data encryption**
  - More stronger encryption
    - 2-phace encryption
  - Encryption for usability
    - Transparent Data Encryption

Innovative R&D by NTT

Planning for TDE Patch

- **Develop Table level TDE function 2steps**
  - Step 1: Basic TDE Module (2018)
  - Step 2: Support in WAL Level (2019)
- **In 2018, I'll post a Table Level TDE function to PG Hackers**
- **This is only basic TDE method**

If you have an interest,
Please Join Discussion and Review

NTT

Question?

Thank you