

# Rancangan Implementasi Manajemen Database pada *Background Process* Menggunakan CrondManager Sebagai Upaya Peningkatan *Performance* dan Keamanan Data Secara *Online*: Studi Kasus PT. YZI

Satria Dwi Putra<sup>1</sup> dan Muhammad Rifqi<sup>2</sup>

Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana<sup>1,2</sup>  
E-mail : satria11t2@gmail.com<sup>1</sup>, rifqi\_muh99@yahoo.co.id<sup>2</sup>

**Abstract--** Processing of data efficiently will adversely impact the live cycle time applications. However, on the other hand the concern related to management and structured data is still lacking, so that such a bad impact of system downtime. This happens because the delivery mechanism for data that does not correspond to the role of business models and applications. PT. YZI is an organization engaged in online advertising property, where each day its ad information obtained in real time both the merchant and independent property agent. However, there are some processes that are found are still not in accordance with the role model PT.YZI include a data management and structure are still lacking that declining application performance and her no data encryption to ensure data security. With the basic theory java native and method AES() encryption MySQL then CrondManager is one of alternative tools of data processing that can be implemented right on the system. The end result of this research is the design implementation process CrondManager the background system for PT. YZI who apply online integration of data in the form of a data listing and/or encryption of data that are proven to meet the data security aspects. By implementing this CrondManager expected aspects of performance systems, data security and zero downtime system can be met.

**Keywords:** Database management, Data Processing, background Processing, Data Security, CrondManager

**Abstrak--** Pengolahan data secara efisien akan sangat berdampak pada siklus *live time* aplikasi. Namun, di sisi lain kepedulian terkait manajemen data yang baik dan terstruktur masih kurang, sehingga berdampak buruk seperti *downtime* sistem. Hal tersebut terjadi karena mekanisme pengiriman data yang tidak sesuai dengan *role model* bisnis dan aplikasi. PT. YZI merupakan organisasi yang bergerak dibidang *online advertising property*, yang mana setiap hari nya informasi iklan didapatkan secara *real time* baik dari *merchant* maupun *agent property independent*. Namun ada beberapa proses yang ditemukan masih tidak sesuai dengan role model PT.YZI antara lain manajemen data dan struktur yang masih kurang sehingga *performance* aplikasi menurun dan tidak ada nya enkripsi data untuk menjamin keamanan data. Dengan teori dasar java native dan metoda enkripsi AES() MySQL maka CrondManager merupakan salah satu alternatif *tools data processing* yang dapat diimplementasi kan pada sistem. Hasil akhir dari penelitian ini berupa rancangan implementasi CrondManager pada sistem *background* proses bagi PT. YZI yang menerapkan *online data integration* berupa data listing dan/atau enkripsi data yang terbukti dapat memenuhi aspek keamanan data. Dengan mengimplementasikan CrondManager ini diharapkan aspek *performance system*, *data security* dan *zero downtime system* dapat terpenuhi.

**Kata Kunci:** Manajemen Database, Pemrosesan Data, Background Processing, Keamanan Data, CrondManager.

## I. PENDAHULUAN

Pengguna internet di seluruh dunia sampai dengan akhir tahun 2016 seperti yang tercatat dalam survei Internet World Stats pada internetworldstats.com mencapai 3.611.375.813 pengguna, dengan statistik tertinggi pengguna dari Asia mencapai 44,2%[1]. Website merupakan salah satu fasilitas internet yang paling sering digunakan di dunia khususnya di Indonesia, karena dengan adanya website pertukaran informasi dan penyebaran informasi dapat dilakukan secara efisien. Bahkan tercatat dari hasil analisis rumah123.com pencarian properti selama kuartal I-2016 meningkat 66 persen dibandingkan periode yang sama pada 2015[2].

Meskipun menjadi sarana transaksi informasi yang handal dan banyak digunakan, mekanisme pengiriman data yang tidak sesuai dengan *role model* sehingga memungkinkan *downtime* sistem dan terjadi nya serangan oleh *digital attacker* seperti pencurian data – data penting. Aspek kerahasiaan data penting seperti lokasi/koordinat , password user dan data penting lain nya dapat dipastikan hanya diakses oleh aplikasi atau *administrator*.

Kendala terkait *zero downtime* sistem dan keamanan data tersebut dapat diatasi dengan teknik kriptografi berbasis proses penjadwalan dengan AES Enkripsi *database* atau yang dikenal dengan CrondManager karena terdapat dua proses yang dilakukan yaitu proses penjadwalan sebagai solusi *zero downtime* sistem dan AES Enkripsi *database* sebagai solusi untuk keamanan data dan sebagai validasi akses aplikasi dan *administartor*.

Penelitian ini bertujuan untuk mendeskripsikan rancangan implementasi CrondManager pada sistem *backgroud* proses PT. YZI, membuktikan aspek siklus *live time* aplikasi dapat terpenuhi dalam memproses data iklan dari merchant maupun dari agent property independent yang menerapkan CrondManager, serta membandingkan keaman data antara sebelum dan sesudah menerapkan CrondManager.

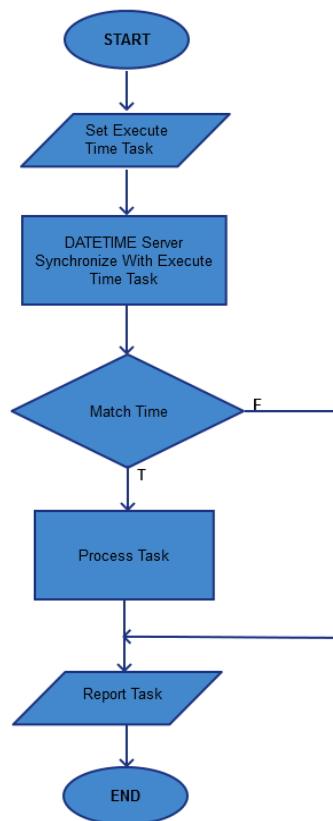
## II. METODOLOGI PENELITIAN

### A. Cron Jobs

Cron Jobs mengakomodir otomatisasi perintah atau script tertentu pada sistem. Perintah atau script dapat diatur penjadwalan nya setiap jam, hari, minggu dan lain – lain. Cron Jobs adalah software yang bertugas untuk penjadwalan yang memungkinkan melakukan task tertentu secara terjadwal [3].

### B. Custom Cron Jobs

Pola yang sudah diterapkan pada Cron Jobs selanjutnya dilakukan optimalisasi pada Custom Cron Jobs dengan menggunakan program Java untuk mengakomodir proses paralel maupun serial. Dengan memanfaatkan mekanisme *Thread* dan *Synchronized* pada bahasa pemrograman Java [4].



Gambar 1. Flow of process Custom Cron Jobs

### C. Varbinary Data Type

Pada dasarnya tipe data Binary dan Varbinary sama dengan Char dan Varchar, perbedaannya hanya pada struktur penyimpanan MySQL, dimana tipe data binary akan disimpan secara biner (bit per bit), bukan secara karakter seperti Char. Sederhananya, hal ini akan berefek pada case-sensitif data (perbedaan penggunaan huruf besar dan huruf kecil). Pada tipe data Char, Jika kita menyimpan data 'A', maka secara internal MySQL akan menyimpannya sebagai karakter 'A', dimana 'A' akan sama dengan 'a'. Namun untuk tipe data Binary, 'A' akan disimpan sebagai bit dari 'A', yaitu 65, dan akan berbeda dengan 'a', dimana nilai binernya adalah 97.

Dimana sama seperti tipe data Char dan Varchar, M adalah jumlah karakter yang akan dialokasikan oleh MySQL menyediakan 5 karakter untuk kolom tersebut. Nilai M maksimal 255 karakter untuk Binary, dan 65.535 karakter untuk Varbinary. Jika nilai M tidak dinyatakan, nilai defaultnya adalah 1. Binary akan disimpan dalam ukuran yang tetap, sedangkan Varbinary akan berubah sesuai ukuran data (sama dengan perbedaan antara Char dan Varchar)[5]. Pemilihan tipe data yang tepat dan sesuai akan meningkatkan *performance* aplikasi,

Contoh query membuat tabel dengan tipe data Varbinary:

```
mysql> CREATE TABLE contoh_bin (bin BINARY(5),
varbin VARBINARY(5));
Query OK, 0 rows affected (0.08 sec)

mysql> INSERT INTO contoh_bin values ('dunia','dunia');
Query OK, 1 row affected (0.04 sec)

mysql> SELECT * FROM contoh_bin;
+-----+-----+
| bin  | varbin |
+-----+-----+
| dunia | dunia  |
+-----+-----+
1 row in set (0.00 sec)

mysql> SELECT * FROM contoh_bin where bin='dunia';
+-----+-----+
| bin  | varbin |
+-----+-----+
| dunia | dunia  |
+-----+-----+
1 row in set (0.00 sec)

mysql> SELECT * FROM contoh_bin where bin='DUNIA';
Empty set (0.00 sec)
```

Query terakhir tidak menampilkan hasil apa – apa karena dalam Binary, ‘dunia’ tidak sama dengan ‘DUNIA’.

**D. Aspek Keamanan Data**

Ada empat aspek utama dalam keamanan data dan dua aspek lain yang saling berkaitan.

1. *Privacy/Confidentiality*  
Usaha menjaga data informasi dari orang yang tidak berhak mengakses (memastikan bahwa data informasi pribadi kita tetap pribadi).
2. *Integrity*  
Usaha untuk menjaga data atau informasi agar tidak diubah oleh orang yang tidak berhak.
3. *Authentication*  
Usaha atau metoda untuk mengetahui keaslian dari informasi, misalnya apakah informasi yang dikirim dibuka oleh orang yang benar (asli) atau layanan dari server yang diberikan benar berasal dari server yang dimaksud.
4. *Availability*  
*Availability* berhubungan dengan ketersediaan informasi ketika dibutuhkan, Data yang diserang atau dijebol dapat mengubah atau meniadakan data yang sudah tersedia.
5. *Access Control*  
*Access Control* berhubungan dengan cara pengaturan akses informasi dan pastinya berhubungan dengan klasifikasi data.
6. *Non-repudiation*  
Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan perubahan data sehingga data yang diberikan valid.

E. Kriptografi

Dalam kriptografi terdapat dua konsep utama yakni enkripsi/dekripsi dan tanda tangan digital.

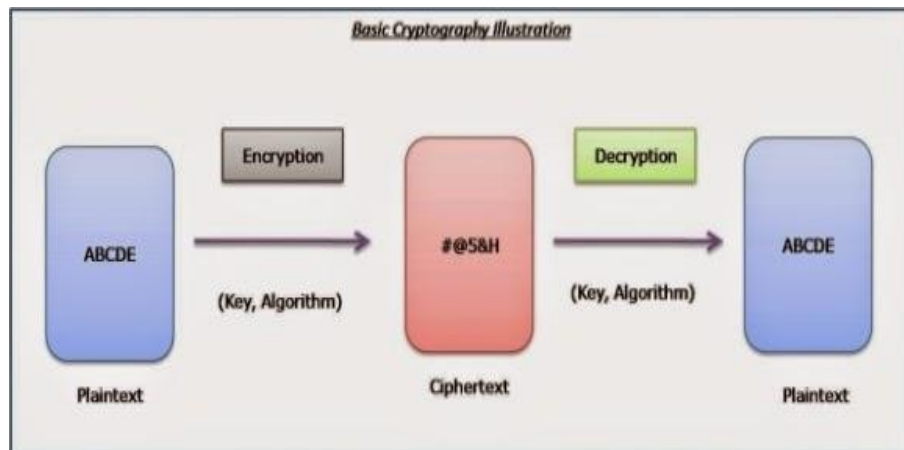
1. Enkripsi/Dekripsi

Enkripsi adalah proses mengolah informasi/data (*plaintext*) menjadi bentuk hampir tidak dikenali (*ciphertext*) dengan menggunakan algoritma tertentu.

Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali *ciphertext* menjadi *plaintext*.

2. Tanda Tangan Digital

Tanda tangan digital adalah suatu nilai kriptografis yang bergantung pada isi berkas digital dan kunci pemilik berkas digital. Tanda tangan (*key*) ini dapat dipasang di dalam berkas digital atau disimpan untuk membuktikan keabsahan tanda tangan digital tersebut. Jika tanda tangan digital otentik, berarti berkas digital masih asli dan pemiliknya adalah orang yang sah dan tidak jika sebaliknya [6].



Gambar 2. Basic Algoritma Enkripsi/Dekripsi

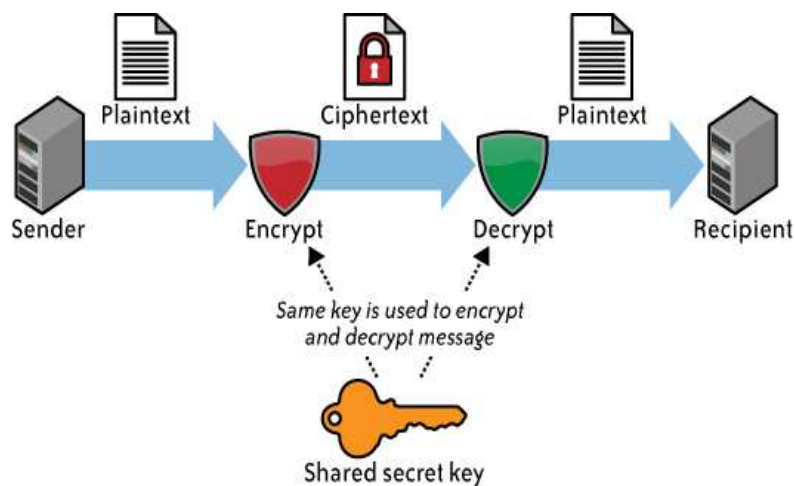
F. MySQL *AES* (*Advanced Encryption Standard*)  
 Terdapat dua fungsi yang disediakan oleh MySQL untuk melakukan Enkripsi/Dekripsi yakni *AES\_ENCRYPT()* dan *AES\_DECRYPT()*.

1. *AES\_ENCRYPT()*

Proses melakukan enkripsi data menggunakan *key\_str* (kunci string) dan mengembalikan data string biner yang berisi output yang telah di enkripsi.

2. *AES\_DECRYPT()*

Proses melakukan dekripsi data yang telah terenkripsi (*crypt\_str*) menggunakan *key\_str* (kunci string) dan mengembalikan data asli/origanal data. Jika data yang terenkripsi adalah *NULL* maka fungsi *AES\_DECRYPT()* akan mengembalikan nilai *NULL*.



Gambar 3. Skema *AES\_ENCRYPT()* dan *AES\_DECRYPT()*

Panjangnya data yang telah dienkripsi dapat dihitung dengan rumus berikut:

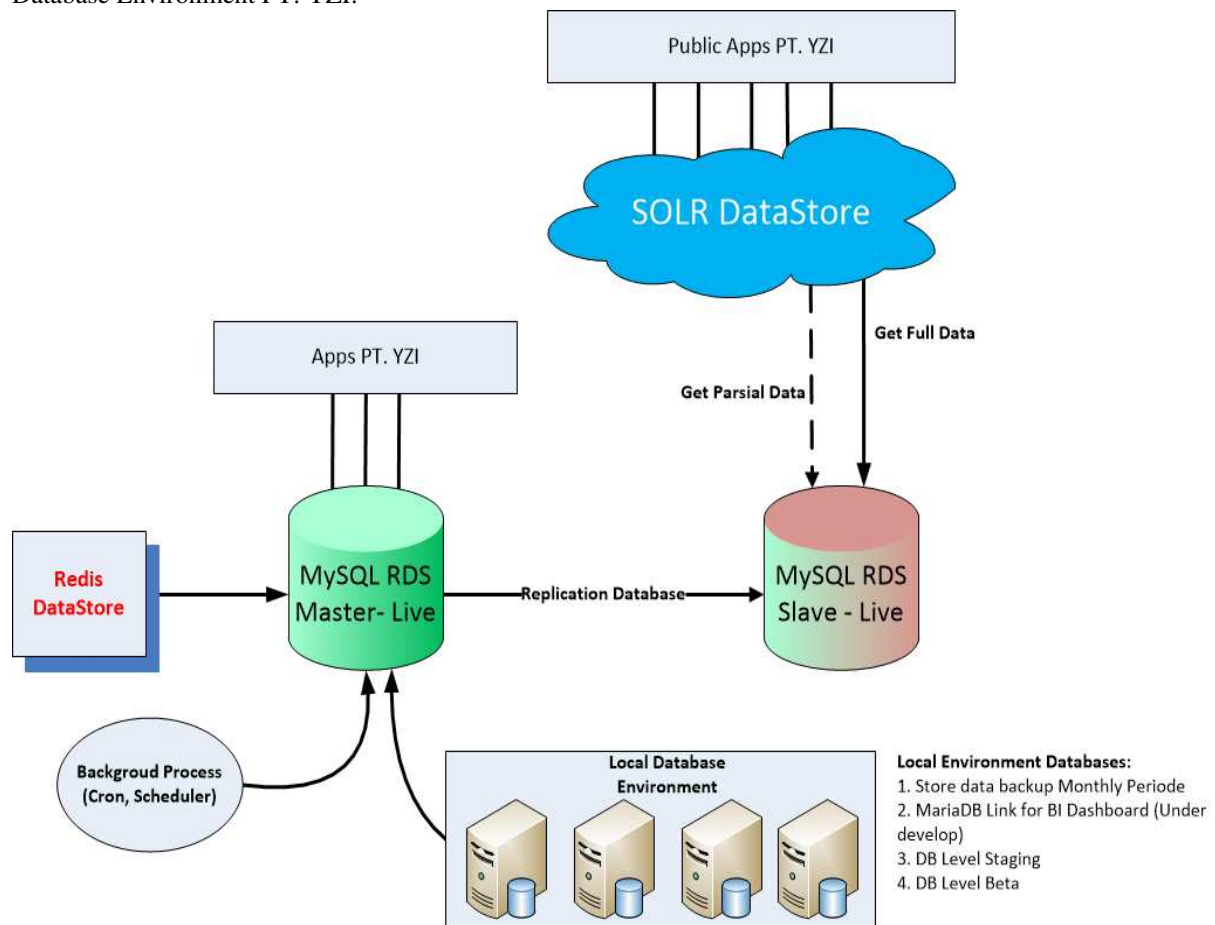
$$16 * (\text{trunc}(\text{string\_length} / 16) + 1)$$

Jika proses dekripsi mendeteksi data yang tidak valid secara otomatis data yang ditampilkan adalah *NULL* [7].

### III. PEKERJAAN DAN DISKUSI HASIL

#### A. Infrastruktur Database Environment PT. YZI

Berdasarkan pengamat peneliti, PT. YZI memiliki infrastruktur environment database yang relatif memadai terlihat dari sangat minimnya terjadi SPOF (*Single Point Of Failure*). Semua environment database production berada pada cloud untuk meningkatkan keamanan data. Untuk lebih jelas nya, berikut gambar Infrastruktur Database Environment PT. YZI:



Gambar 4. Infrastruktur Database Environment PT. YZI.

#### B. Proses CrondManager Mengolah Data

Proses pengolahan data oleh CrondManager (*Custom Crond*) yang dilakukan di PT. YZI saat ini dimonitoring oleh tim DBA (*Database Administrator*). Tim DBA akan mengenerate crond code yang disimpan di *database* dan menentukan interval proses akan berjalan. Tabel 1. berisi daftar crond code yang ada.

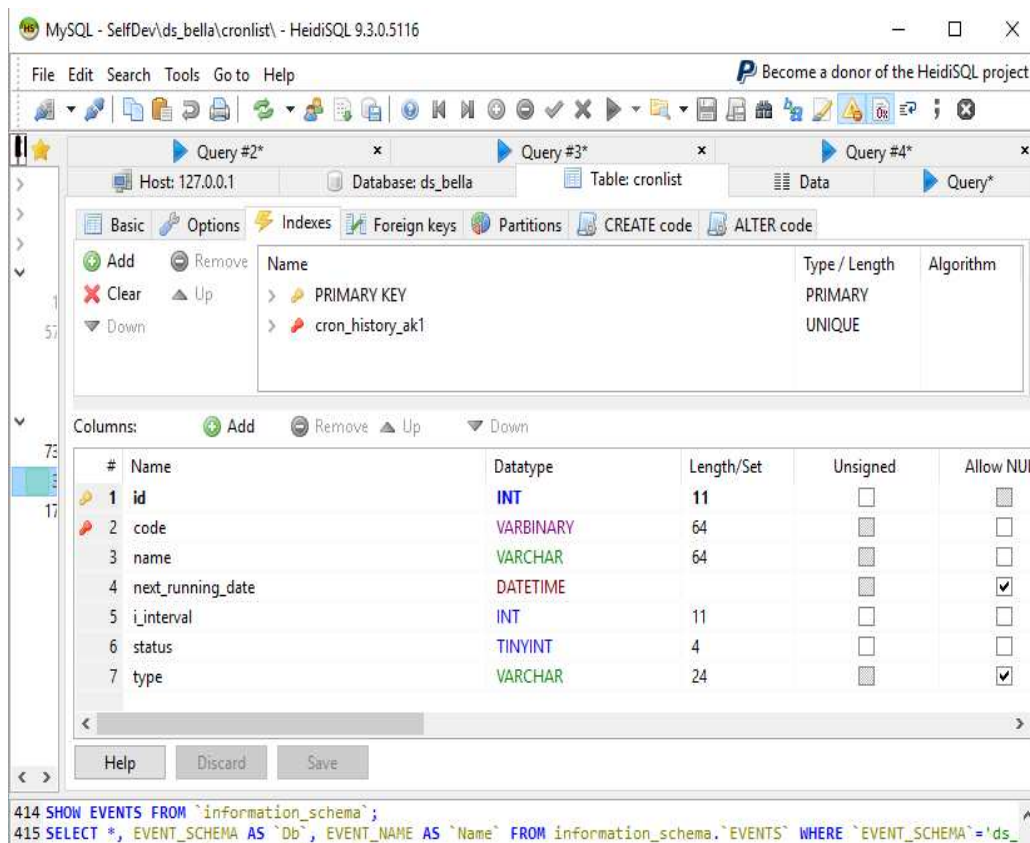
TABEL I  
DAFTAR CRON CODE

name	interval	status	type
Generate commercial listing hit by API	24	Active	Cleaner
Generate house listing hit by API	24	Active	Cleaner
Generate land listing hit by API	24	Active	Cleaner
Alert Expired Listing	24	Active	Generator
FeaturedDeveloper	24	Disable	Generator
user_recent_search cleaner	24	Active	Cleaner
Generate StatisticHitApi	168	Disable	Generator
Generate Daily KPI	24	Active	Generator
Generate Daily Company User Summary	24	Active	Generator

Alur proses *generate code* inilah yang diterapkan PT. YZI pada database menggunakan enkripsi dan dekripsi. Alasan PT. YZI menggunakan proses enkripsi dan dekripsi adalah sebagai berikut :

1. PT. YZI telah memiliki infrastruktur yang berada pada *cloud*.
2. Untuk meningkatkan keamana pada *cloud* karena Database server berada pada satu *group cloud* (Meningkatkan autentikasi user).
3. Keamanan data yang sangat valid karena hanya orang yang sah yang mengetahui secret key.
4. Public apps PT. YZI akan sangat aman dari pencurian data.
5. Manajemen Database yang terstruktur dan terdokumentasi sehingga minim dengan human error.

Berikut deskripsi tabel yang digunakan untuk mengenerate code, crond code disimpan dengan tipe data Varbinary pada *field code* :



Gambar 5. Field code dengan tipe data varbinary.

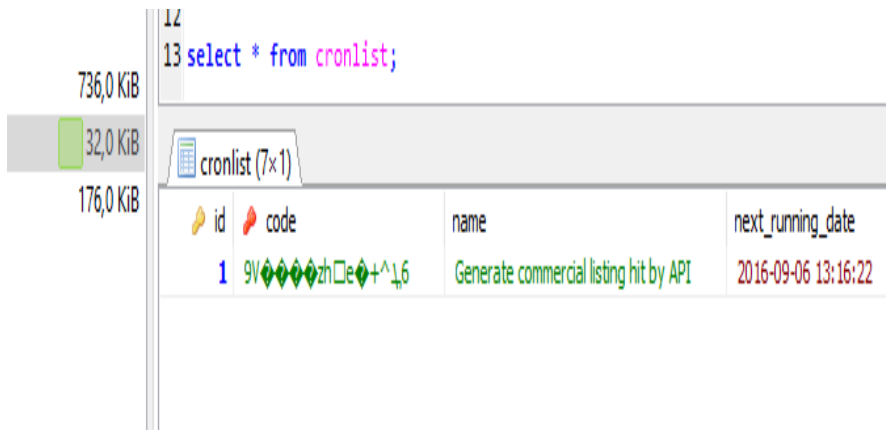
### C. Proses Enkripsi/Dekripsi Code

Ketika mengenerate code tim DBA akan menentukan secret key yang mana secret key akan digunakan oleh CrondManager untuk melakukan Dekripsi agar kembali ke data semula/original data.

Berikut query generete code dengan Enkripsi:

```
INSERT INTO cronlist
(id,code,name,next_running_date,i_interval,status,type)
VALUES
(1,AES_ENCRYPT('StatHitAPIcom','MrSapiSuper777'),
'Generate commercial listing hit by
API',NOW(),24,1,'Cleaner');
```

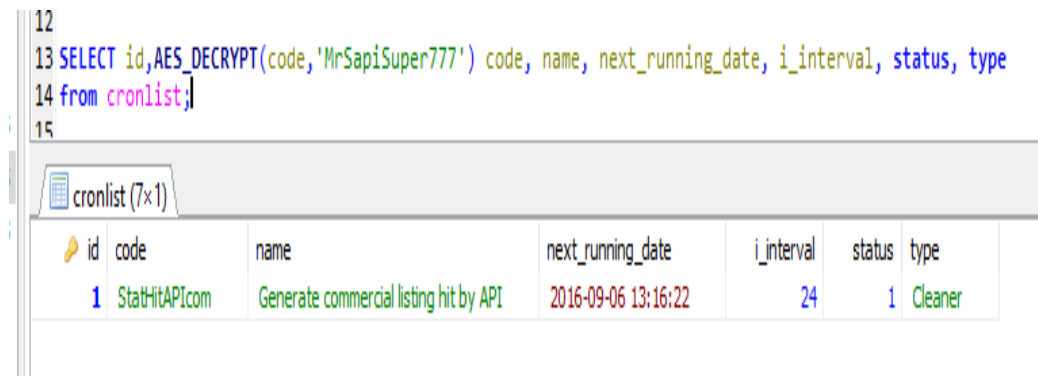
Nilai data yang di enkripsi adalah 'StatHitAPIcom' dengan secret key 'MrSapiSuper777' data tersebut akan ditempatkan pada field code dengan tipe data varbinary. Berikut hasil nya :



Gambar 6. Data pada Field code yang di enkripsi.

Untuk melakukan dekripsi cukup menggunakan fungsi AES\_DECRYPT() dengan menggunakan secret key yang sama yaitu 'MrSapiSuper777'. Berikut contoh query dan result yang ditampilkan :

```
SELECT id,AES_DECRYPT(code,'MrSapiSuper777') code, name, next_running_date,
i_interval, status, type
from cronlist;
```



Gambar 7. Data pada Field code yang di dekripsi.

Dekripsi pada sisi aplikasi CrondManager yang sudah di implementasikan pada backend process. Gambar 8 menunjukkan bahwa script status menampilkan proses code yang telah di dekripsi dan mengetahui status proses setiap proses CrondManager.

```

Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^'.
Welcome to Cron Console Monitoring
Running version [1.0]
(C) Copyright 2015

CRONMON >status
(.) MembershipListReportV2 [1] [2016-09-06 19:05:00] [success]
(.) NewPropertyModifyStatus [24] [2016-09-07 14:10:00] [success]
(.) AreaOfListingOnline [3] [2016-09-06 21:30:00] [success]
(.) UserListingSummary [1] [2016-09-06 19:35:00] [success]
(.) QcListingGenerator [24] [2016-09-07 06:00:00] [No Schedule QC Listing]
(.) EmrciesFileGenerator [24] [2016-08-31 21:50:12] [0]
(.) CategoryOFDirectory [1] [2016-09-06 19:10:00] [success]
(.) NewThematicListing [24] [2016-09-07 18:14:48] [success]
(.) DirectoryModifyStatus [24] [2016-09-06 22:45:00] [success]
(.) UserListingSummaryV2 [1] [2016-09-06 19:38:00] [success]
(.) TagListSummary [24] [2016-09-07 15:45:00] [success]
(.) MarketTrendWeeklyArea [168] [2016-09-12 04:00:00] [success]

CRONMON_>

```

Gambar 8. Data pada Field code yang di dekripsi

#### IV. KESIMPULAN

Dari uraian yang telah dipaparkan, dapat diambil kesimpulan bahwa teknologi custom crond (CrondManager) dengan metoda enkripsi/dekripsi AES MySQL merupakan solusi alternatif yang sesuai bagi PT. YZI untuk meningkatkan Keamanan Data secara Online dan *Performance* aplikasi karena pemilihan tipe data yang tepat dan sesuai.

Saat ini PT. YZI telah memiliki infrastruktur database *environment* yang berada di cloud yang nantinya dapat mengimplementasikan teknologi enkripsi/dekripsi AES MySQL dari sisi *Front-end*.

Dari hasil implementasi yang dilakukan oleh peneliti, didapatkan bahwa proses enkripsi/dekripsi data dapat sukses dilakukan di *environment production*. Hal ini dapat terlihat dari berhasilnya data – data penting terenkripsi dan terdekripsi dengan baik. Aspek – aspek keamanan informasi yang meliputi *Privacy*, *Integrity*, *authentication* dan *non-repudiation* dapat terpenuhi oleh teknologi CrondManager dengan metoda enkripsi/dekripsi AES MySQL. Hal ini didapatkan dari hasil pengujian keamanan yang telah dilakukan oleh peneliti. Dari tingkat keamanan data lebih terjamin dari *Data fraud* dikarenakan seluruh data yang ditransaksikan akan dienkripsi dan didekripsi oleh CrondManager.

#### IV. DAFTAR PUSTAKA

- [1] Internet World Stats. 2016. *Internet Usage Statistics*. <http://www.internetworldstats.com/stats.htm> . 01 September 2016.
- [2] Rumah123.com. 2016. Analisis Pencarian Properti. <http://www.rumah123.com/artikel/ada-peningkatan-transaksi-properti-di-rumah123-com-28561>. 01 September 2016.
- [3] idcloudhost.com. 2016. Kenali Apa itu Cron Jobs ?. <https://idcloudhost.com/kenali-apa-itu-cron-jobs/>. 02 September 2016.
- [4] Docs Oracle Java. 2015. *Synchronized Methods*. <https://docs.oracle.com/javase/tutorial/essential/concurrency/syncmeth.html>. 02 September 2016.
- [5] Andre. 2012. Tipe Data Binary dan Varbinary dalam MySQL. <http://www.duniaikom.com/tutorial-mysql-tipe-data-huruf-char-varchar-text/>. 02 September 2016.
- [6] Radianta, Veriztiarta. 2015. Pengamanan Data Kriptografi dan Steganografi Berserta Penjelasannya. <http://begal-tech.blogspot.co.id/2015/11/pengamanan-data-pengertian-kriptografi-dan-steganogarf.html>. 06 September 2016.
- [7] MySQL Dev. 2005. *Encryption and Compression Functions*. <http://dev.mysql.com/doc/refman/5.7/en/encryption-functions.html>. 06 September 2016.