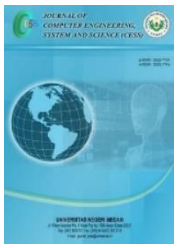
CESS
(Journal of Computing Engineering, System and Science)
e-ISSN: 2502-714x
p-ISSN: 2502-7131

Contents list available at www.jurnal.unimed.ac.id

CESS
(Journal of Computing Engineering, System and Science)

journal homepage: https://jurnal.unimed.ac.id/2012/index.php/cess



Replikasi Database Dengan Sistem Pengamanan Kriptografi Triangle Chain

Database Replication With Security System Triangle Chain Cryptography

Muhammad Affansyah Tanjung[1], Dodi Siregar[2], Mufida Khairani[3]

[1,2,3] *Universitas Harapan Medan*
Jl. HM Joni No 70 C Medan
email: [1] m.affansyah30@gmail.com, [2] dodi.stth@gmail.com, [3] mufida.khairani@gmail.com

A B S T R A K

Basis data merupakan salah satu komponen pembentuk sistem informasi. Saat ini informasi telah menjadi suatu kebutuhan yang penting bagi masyarakat. Serta Kebutuhan akan sistem informasi atau data yang semakin meningkat menjadikan data menjadi aset yang bernilai tinggi. Kemampuan untuk mengakses dan menyediakan informasi secara tepat dan akurat menjadi penting bagi pengguna. Pentingnya informasi menyebabkan perlu dilakukan pengamanan terhadap informasi untuk menjaga keabsahan dan nilai yang dimiliki oleh informasi tersebut, agar tidak disalahgunakan oleh pihak lain yang tidak bertanggungjawab. Dengan demikian penting untuk menjaga data agar tetap ada kapan saja dibutuhkan. Akan tetapi resiko terjadinya kerusakan (*failure*) pada database yang mengakibatkan data tidak dapat diakses atau bahkan mengakibatkan data loss dapat terjadi setiap saat. Gangguan tersebut dapat berupa maintenance, kerusakan database, kerusakan media dan data corruption. Adapun teknik penyelamatan data yang dilakukan, yaitu replikasi database. Replikasi merupakan suatu teknik untuk melakukan copy dan pendistribusian data dan objek-objek database dari satu database ke database lain dan melaksanakan sinkronisasi antara database sehingga konsistensi data dapat terjamin. Pada umumnya, suatu sistem informasi mempunyai database yang dilengkapi dengan keamanan, yaitu berupa password bagi administrator. Tetapi jika password tersebut bisa diketahui atau dipecahkan oleh orang lain maka isi database yang mungkin bersifat rahasia dapat dibaca oleh orang lain yang tidak berkepentingan untuk membacanya. Untuk tujuan keamanan tersebut maka perlu dilakukan enkripsi pada record database menggunakan algoritma Triangle Chain. Hasil pengujian model replikasi asynchronous pada database MySQL dengan pengamanan algoritma kriptografi Triangle Chain dapat menjaga ketersediaan data tetap valid dan konsisten serta meningkatkan keamanan pada replikasi database, karena setiap record data pada tabel database akan terlebih dahulu dienkripsi sebelum direplikasi ke database slave sehingga dapat melindungi dari gangguan maupun serangan dari pihak yang tidak bertanggung jawab.

**Penulis Korespondensi:*
email: emailkorespondensi@gmail.com

Kata Kunci: *Replikasi, Database, Kriptografi, Triangle Chain.*

A B S T R A C T

The database is one of the components that make up the information Systems. Nowadays, information has become an important need for society. As well as the need for an information system or database that is increasing, making data a high-value asset. The ability to access and provide precise and accurate information is important for users. The importance of information makes it necessary to secure the information to maintain the validity and value of the information, so that it is not misused by other irresponsible parties. Thus it is important to keep the data available whenever needed. The data rescue technique used is database replication. Replication is a technique for copying and distributing data and database objects from one database to another database and synchronizing between databases so that data consistency can be guaranteed. In general, an information system has a database that is equipped with security, which is a password for administrators. But if the password can be known or solved by someone else then the contents of the database that may be confidential can be read by other people who are not interested to read it. For security purposes, it is necessary to encrypt the database record. to minimize problems with the database by encoding database table records using the Triangle Chain algorithm. The results of testing the asynchronous replication model on a MySQL database with the security of the Triangle Chain cryptographic algorithm can maintain valid and consistent data availability and increase security in database replication, because each data record in the database table will first be encrypted before being replicated to the slave database so that it can protect from interference. as well as attacks from irresponsible parties.

Keywords: *Replication, Database, Cryptography, Triangle Chain.*

1. PENDAHULUAN

Kebutuhan akan sistem database yang semakin meningkat menjadikan data menjadi aset yang bernilai tinggi. Sistem database (*basis data*) adalah sistem komputerisasi yang tujuan utamanya adalah memelihara informasi dan membuat informasi tersebut tersedia saat dibutuhkan suatu field terhadap record-record yang sejenis, sama besar, sama bentuk dan merupakan sekumpulan entity yang seragam [1]. Dalam jaringan komputer, database merupakan sebuah pondasi atau sesuatu yang harus diikutsertakan. Dengan demikian penting untuk menjaga data agar tetap aman dan ada kapan saja dibutuhkan. Akan tetapi resiko terjadinya kerusakan (*failure*) pada database yang mengakibatkan data tidak dapat diakses atau bahkan mengakibatkan kehilangan data dapat terjadi setiap saat. Gangguan tersebut dapat berupa maintenance atau kerusakan database.

Adapun teknik penyelamatan data yang sering dilakukan, yaitu backup data. Backup data merupakan teknik menyalin data ke dalam media lain. Namun demikian hal ini belum dapat menjadi solusi terbaik karena backup tidak menggantikan kinerja primary database secara langsung yang mengakibatkan data tidak dapat diakses sampai maintenance pada sistem primary database tersebut berakhir. Oleh karena itu teknik replikasi dapat menjadi solusi keefektifan dalam menjawab kekurang praktisan proses backup data. Replikasi database adalah suatu teknik untuk melakukan copy dan pendistribusian data dan objek-objek database dari satu database ke database lain dan melaksanakan sinkronisasi antara database

sehingga konsistensi data dapat terjamin [2]. Dengan menggunakan teknik replikasi ini, data dapat didistribusikan ke lokasi yang berbeda melalui koneksi jaringan lokal maupun internet.

Keamanan database juga perlu dijaga terhadap berbagai bentuk ancaman dan gangguan, baik yang bersifat teknis maupun administrasi. Secara keseluruhan, gangguan terhadap database baik fisik maupun nonfisik, meliputi pencurian data serta hilangnya kerahasiaan data. Untuk itulah diperlukannya pengamanan data dengan menggabungkan teknik kriptografi pada sistem replikasi database. Kiptografi merupakan sebuah teori keamanan untuk menjaga kerahasiaan pesan dengan cara menyandikan ke dalam bentuk yang tidak dapat dimengerti orang lain, selain pemilik data tersebut [3]. Penerapan kriptografi bertujuan untuk mengenkripsi record database, sedangkan replikasi database bertujuan untuk menduplikat database. Jika salah satu database ada yang rusak masih terdapat database duplikatnya atau jika salah satu database dicuri orang lain maka masih tersedia keamanan tambahan yaitu nilai (*value*) pada database yang terenkripsi, sehingga database masih terjaga kerahasiaanya terhadap orang yang tidak berkepentingan untuk membacanya.

Berdasarkan uraian pada latar belakang yang sudah dijelaskan, maka penulis melakukan penelitian yang dituangkan dalam bentuk skripsi. Penelitian ini penulis beri judul "Replikasi Database Dengan Sistem Pengamanan Kriptografi Triangle Chain". Penelitian ini diharapkan dapat dijadikan sebagai salah satu solusi yang dapat menangani keamanan database dan kehilangan data, sehingga data tetap aman dapat diakses kapan saja oleh user.

2. DASAR TEORI

Pada penelitian replikasi database dengan sistem pengamanan kriptografi Triangle Chain penulis akan mengungkapkan referensi kajian pustaka. Pustaka yang relevan digunakan dan menjadi acuan bagi penulis dalam menyusun dan melakukan penelitian.

2.1. Replikasi Database

Dalam penggunaan data secara bersama diperlukan suatu metode untuk mendistribusikan data. Salah satu cara pendistribusian database yaitu dengan menggunakan replikasi database. Replikasi adalah pengoperasian menyimpan bagian dari database, sebagai salinan, pada beberapa node pada sebuah jaringan [4]. Menurut [5], replikasi adalah teknik penggandaan data pada beberapa lokasi fisik yang berbeda untuk satu data logic yang sama. Kegiatan ini bertujuan apabila terjadi kerusakan atau kegagalan pada satu lokasi fisik tidak akan mempengaruhi kinerja seluruh sistem.

Replikasi database juga dapat digunakan dalam hal meningkatkan availabilitas sistem database dengan cara membagi beban pekerjaaan pada tiap database server. Berdasarkan jenis replikasi, Reeplikasi dibedakan menjadi dua bagian yaitu replikasi synchronous dan replikasi asynchronous. Adapun perbedaan darikedua replikasi ini adalah sebagai berikut:

1. Replikasi Synchronous
   a. Proses replikasi terjadi secara real time
   b. Sinkronisasi data menyediakan recovery data yang konsisten
   c. Proses penulisan pada master dan slave harus selesai terlebih dahulu sebelum beralih ke transaksi berikutnya.
   d. Keuntungannya yaitu menyediakan recovery yang konsisten karena sinkronisasi data terjaga.
2. Replikasi Asynchronous

a. Proses replikasi tidak berjalan secara realtime. Data akan diletakan dalam sebuah buffer terlebih dahulu setelah itu dalam jangka waktu tertentu akan di replikasi ke slave.
b. Apabila terjadi crash pada salah satu node saat replikasi belum selesai, data hasil replikasi tidak dapat dipastikan telah identik.
c. Setelah transaksi di master selesai barulah proses replikasi berlangsung.
d. Keuntungannya yaitu efektifitas biaya proses transaksi.

Keuntungan replikasi tergantung dari jenis replikasi tetapi pada umumnya replikasi mendukung ketersediaan data setiap waktu dan dimanapun diperlukan. Adapun keuntungan lainnya yaitu memungkinkan beberapa lokasi menyimpan data yang sama. Hal ini sangat berguna pada saat lokasi-lokasi tersebut membutuhkan data yang sama atau memerlukan server yang terpisah dalam pembuatan aplikasi laporan dan Pengguna dapat bekerja dengan meng-copy data pada saat tidak terkoneksi kemudian melakukan perubahan untuk dibuat database baru pada saat terkoneksi [6].

2.2. Algoritma Kriptografi Triangle Chain

Kiptografi merupakan sebuah teori keamanan untuk menjaga kerahasiaan pesan dengan cara menyandikan ke dalam bentuk yang tidak dapat dimengerti orang lain, selain pemilik data tersebut [3]. Tujuan dari kriptografi adalah untuk tidak menyembunyikan keberadaan pesan, melainkan untuk menyembunyikan maknanya [7]. Algoritma dalam kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang lain yang tidak berhak atas pesan tersebut. Pada penelitian ini menggunakan algoritma Triangle Chain yang merupakan jenis algoritma simetris, dimana kunci yang digunakan untuk proses enkrips dan dekripsi adalah sama.

Algoritma Triangle Chain atau umumnya dikenal dengan sebutan algoritma rantai segitiga merupakan cipher yang ide awalnya dari algoritma kriptografi One Time Pad, yaitu kunci yang dibangkitkan secara random dan panjang kunci sepanjang plaintext yang akan dienkripsi. Algoritma kriptografi Triangle Chain membangkitkan kunci-kunci secara otomatis dilakukan dengan teknik berantai. Kekuatan cipher ini terletak pada kunci, yaitu nilai integer yang menunjukkan pergeseran karakter-karakter sesuai dengan operasi pada Caesar Cipher. Kekuatan kedua terletak pada barisan bilangan-bilangan yang berfungsi sebagai pengali dengan kunci [8].

Proses enkripsi dan dekripsi pada algoritma Triangle Chain dilakukan secara berantai berdasarkan perkalian nilai kunci dan factor pengali yang dilakukan secara ganda sehingga hasil yang didapat jauh berbeda dengan pesan asli [9]. Secara matematis pola enkripsi rantai segitiga dapat digambarkan dengan matriks N x N dengan N merupakan panjang plainteks yang akan dienkripsi dan operasi pada alfabet ASCII. Matriks dilambangkan dengan Mij, dengan 1 ≤ i ≤ N dan 1 ≤ j ≤ N, nilai integer kunci dengan K, faktor pengali merupakan tabel integer R. Plainteks dengan P dimana P merupakan tabel plainteks dengan panjang N yaitu P[N]. Adapun algoritma enkripsi yang ada pada Triangle Chain [10] dengan menggunakan rumus sebagai berikut:

1. Matriks enkripsi segitiga pertama

untuk baris ke-1 :

$$M_{[ij]} = P[j] + (K * R[1] \text{Mod } 256 \qquad (1)$$

untuk baris ke-2 dan selanjutnya untuk nilai $j \geq i$

$$M_{[ij]} = M_{[i-1]j} + (K * R[i] \text{Mod } 256 \qquad (2)$$

sehingga nilai ciphertext yang diperoleh adalah :

$M_{[i,j]}$ pada nilai $j = (N + i) - N$

2. Matriks enkripsi segitiga kedua
   nilai P diperoleh dari nilai $M_{[i,j]}$ pada $i = j$
   untuk baris ke-1 :

$$M_{[1j]} = P[j] + (K * R[1]) \text{Mod } 256 \quad (3)$$

   untuk baris ke 2 dan selanjutnya untuk nilai $j \leq (N + 1) - i$

$$M_{[ij]} = M_{[i-1]j} + (K * R[i] \text{Mod } 256 \quad (4)$$

   sehingga nilai ciphertext yang diperoleh adalah :
   $M_{[i,j]}$ pada nilai $j = (N + 1) - i$
   Keterangan :
   - P : Plaintext
   - N : Jumlah karakter plaintext
   - M : Matriks penampung hasil penyandian
   - K : Kunci
   - R : Row (*baris perkalian faktor pengali dengan kunci*)
   - i : Indeks faktor pengali
   - j : Indek karakter plaintext

Sedangkan untuk proses dekripsi merupakan kebalikan dari proses enkripsi yaitu mengembalikan ciphertext kebentuk aslinya (*plaintext*). Berikut operasi matriks untuk proses dekripsi algoritma Triangle Chain [10], yaitu sebagai berikut:

1. Matriks dekripsi segitiga pertama operasinya merupakan kebalikan dari matriks enkripsi, jadi operasi ini kebalikan operasi matriks enkripsi segitiga kedua. Nilai C merupakan tabel dari ciphertext dengan panjang N yaitu C[N].
   untuk baris ke-1, berlaku formula :

$$M_{[1j]} = C[j] - (K * (R[1])) \text{Mod } 256 \quad (5)$$

   sedangkan untuk baris kedua dan selanjutnya dimana nilai $j \leq (N + 1) - i$, berlaku formula :

$$M_{[ij]} = M_{[i-1]j} - (K * (R[i])) \text{Mod } 256 \quad (6)$$

   sehingga nilai plaintext yang diperoleh adalah :
   $M_{[ij]}$ pada nilai $i = n$ dan $j \leq (N + 1) - i$
2. Matriks dekripsi segitiga kedua
   untuk baris pertama berlaku formula :

$$M_{[1j]} = C[j] - (K * (R[1])) \text{Mod } 256 \quad (7)$$

   sedangkan untuk baris kedua dan seterusnya nilai $j \geq i$, berlaku formula :

$$M_{[ij]} = M_{[i-1]j} - \big(K * (R[i])\big) \text{Mod } 256 \quad (8)$$

   sehingga nilai plaintext yang diperoleh adalah :
   $M_{[ij]}$ pada nilai $j = (N + i) - N$
   Keterangan :
   - C : Ciphertext
   - N : Jumlah karakter ciphertext
   - M : Matriks penampung hasil cipher yang dijadikan sebagai plaintext
   - K : Kunci
   - R : Row (*baris perkalian faktor pengali dengan kunci*)
   - i : Indeks faktor pengali
   - j : Indek karakter ciphertext

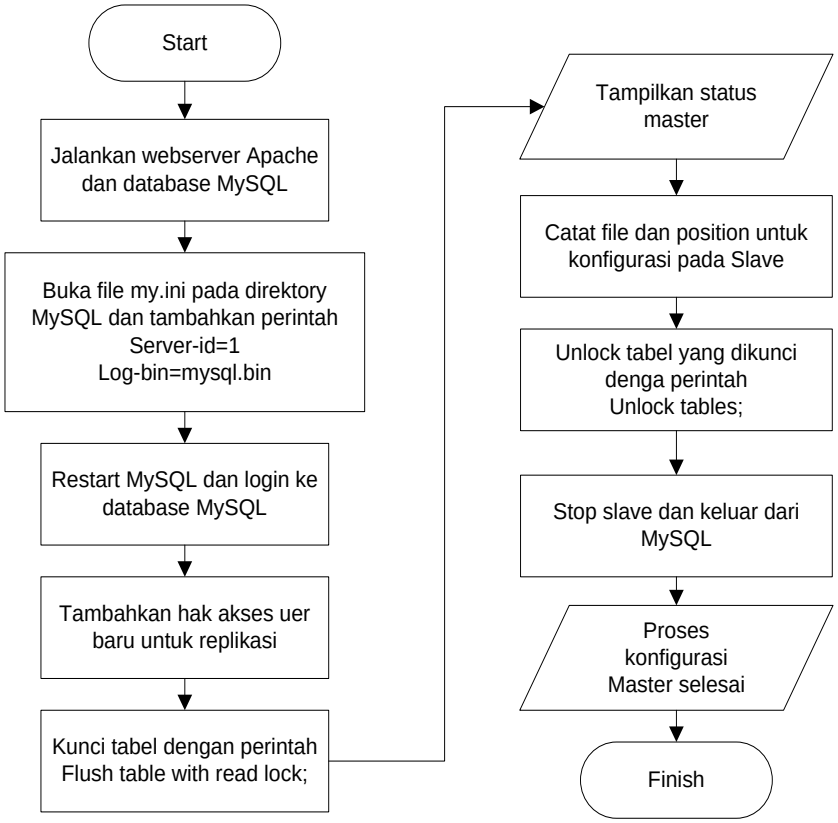
3. METODE PENELITIAN

Model replikasi database yang digunakan dalam penelitian ini yaitu model asynchronous dimana terdapat dua buah komputer yang menjadi database server. Untuk replikasi asynchronous pada basis data MySQL yaitu dimana salah satu ada yang bertindak sebagai komputer master dan yang lain sebagai komputer slave, Untuk cara kerja replikasi nantinya apabila data yang di komputer master dirubah maka otomatis dikomputer slave juga akan berubah, dan begitu juga sebaliknya. Gambar 1 menunjukkan arsitektur jaringan yang penulis gunakan untuk menerapkan konsep replikasi database dengan menggunakan model asynchronous.

Gambar 1. Arsitektur Jaringan Master-Slave Server

Berdasarkan gambar 1 diasumsikan untuk IP komputer master adalah (192.168.1.1), untuk komputer slave adalah (192.168.1.2) dimana kedua komputer pada jaringan dihubungkan dengan menerapkan konsep jaringan host-to-host dengan menggunakan kabel UTP.

Setelah melakukan konfigurasi antara masing-masing komputer maka tahap selanjutnya yaitu melakukan konfigurasi pada database master. Proses replikasi database pada sisi server dapat dijelaskan dalam bentuk flowchart seperti terlihat pada gambar 2.

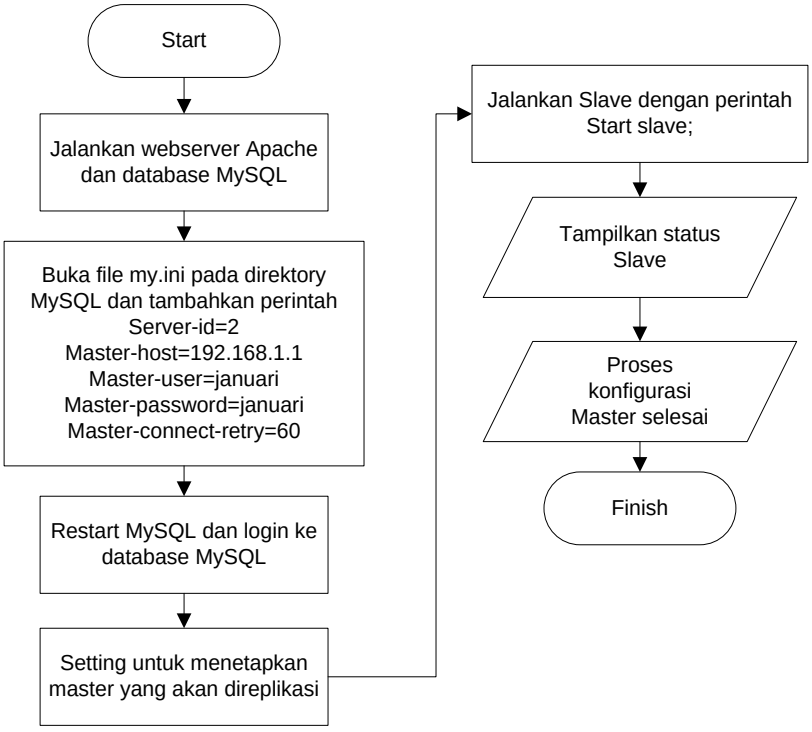


Gambar 2. Flowchart Replikasi Database Pada Server

Berikut tahapan-tahapan konfigurasi replikasi database pada server master dapat diuraikan sebagai berikut:

1. Masuk kedalam direktori C:/xampp/mysql/bin/my.ini kemudian cari [*mysqld*] dan tambahkan query:
   server-id=1
   log-bin=mysql-bin
2. Simpan file konfigurasi MySQL tadi kemudian restart MySQL. Masuk ke command prompt dan login ke MySQL dengan menjalankan query:
   mysql> mysql –u root –p {password user}
3. Berikan hak akses pada slave untuk dapat melakukan replikasi dengan cara membuat user baru dan password pada master, jalankan query:
   *mysql> grant replication slave on *.* to 'user'@'%' identified by 'user';*
4. Kunci tabel dengan menjalankan query:
   flush tables with read lock;
5. Lihat status master yang nantinya akan berguna pada komputer slave. Jalankan perintah berikut untuk melihat status master dengan menjalankan query:
   mysql> show master status;
   catat nama file dan position yang akan digunakan untuk konfigurasi selanjutnya. Unlock tabel yang yang tadi dikunci dengan menjalankan query:
   mysql> unlock tables;
6. Langkah terakhir stop slave dan keluar dari MySQL dengan menjalankan query berikut
   mysql> stop slave;
   quit;

Setelah konfigurasi master berhasil dilakukan maka tahap selanjutnya yaitu melakukan konfigurasi pada slave. Proses replikasi database pada sisi slave dapat dijelaskan dalam bentuk flowchart seperti terlihat pada gambar 3.



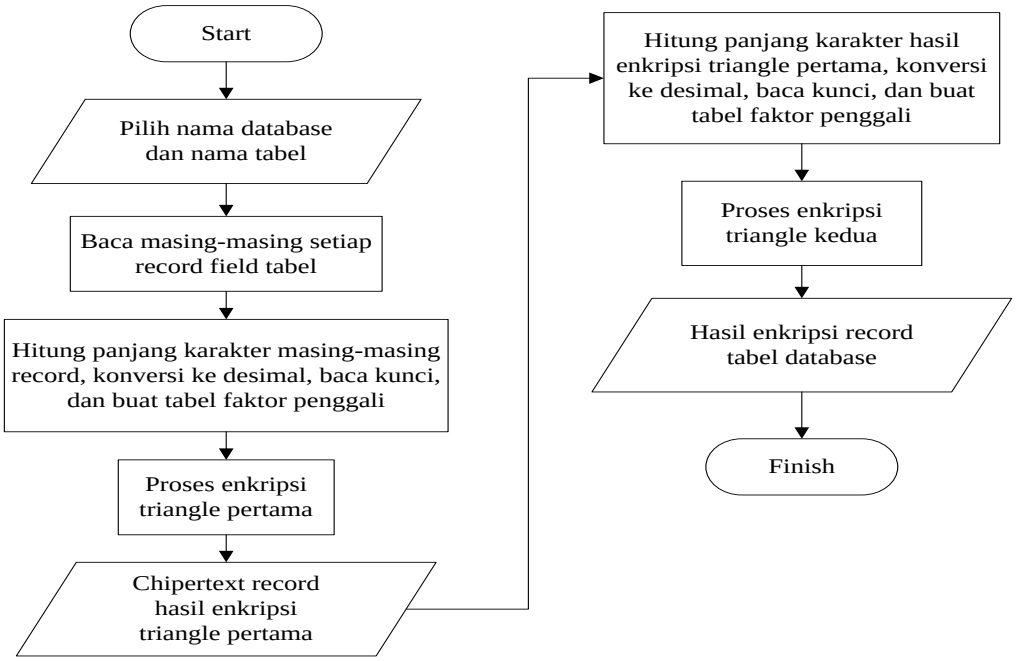
Gambar 3. Flowchart Replikasi Database Pada Slave

Berikut tahapan-tahapan konfigurasi replikasi database pada server slave dapat diuraikan sebagai berikut:

1. Masuk kedalam direktori C:/xampp/mysql/bin/my.ini kemudian cari [*mysqld*] dan tambahkan query:
   server-id=2
   master-host=192.168.1.1
   master-user=januari
   master-password=januari
   master-connect-retry=60
2. Simpan file konfigurasi MySQL tadi kemudian restart MySQL. Masuk ke command prompt dan login ke MySQL dengan menjalankan query:
   mysql> mysql –u root –p {password user}
3. Setting untuk menetapkan master yang akan direplikasi dengan query berikut:
   mysql> change master to master_host '192.168.1.1',
   master_user='januari',
   master_password='januari',
   master_log_file={nama log file},
   master_log_pos={posisi log file};
   master_host diisi dengan ip master, master_user diisi dengan username/pengguna yang akan direplikasi, master_password diisi dengan password dari pengguna master-nya, master_log_file diisi dengan nama file di master yang didapatkan sebelumnya, master_log_pos diisi dengan position dari file-nya.
4. Selanjutnya lakukan start slave pada master dengan menjalankan query:
   mysql> start slave;
5. Lihat status slave apakah sudah tersambung atau belum dengan menjalankan query:
   mysql> show slave status\G

Proses replikasi database adalah proses yang utama atau kunci dari dalam penelitian ini, oleh karena itu dalam proses pendistribusian ini harus dilakukan dengan benar, sehingga prinsip dari replikasi ini benar-benar bisa diterapkan. Pada algoritma Triangle Chain menjelaskan mengenai proses atau langkah-langkah yang dilakukan dalam melakukan enkripsi dan dekripsi record tabel database setelah replikasi database berhasil.

Sebelum proses enkripsi record dilakukan, terlebih dahulu setiap karakter dari record harus dikonversi ke dalam bilangan desimal sesuai dengan nilai-nilai pada tabel ASCII. Hal kedua yang dilakukan adalah pembacaan nilai kunci dan pembentukan tabel faktor pengali, selanjutnya proses enkripsi record dilakukan. Nilai kunci yang digunakan merupakan bilangan integer positif (*bukan nol*), serta barisan bilangan pengali dapat menggunakan bilangan integer asli. Adapun proses enkripsi record tabel database menggunakan algoritma Triangle Chain dapat dijelaskan dalam bentuk flowchart seperti terlihat pada gambar 4.



Gambar 4. Flowchart Enkripsi Record Database Algoritma Triangle Chain

Berdasarkan gambar 4 proses enkripsi dilakukan dengan dua tahap yaitu enkripsi triangle pertama dan enkripsi triangle kedua, sehingga dihasilkan ciphertext akhir yang nantinya menjadi record database. Penyelesaian tahap enkripsi di atas dapat diuraikan melalui contoh kasus penyandian sebuah record di bawah ini:

Plaintext	A	F	A	N
Nilai Desimal	65	70	65	78
Kunci	2 (*bilangan asli integer*)			

Jumlah deret bilangan akan disesuaikan dengan jumlah banyaknya karakter dari plaintext. Jadi, jumlah karakter plaintext (N) adalah 4. Deret bilangan asli (R) yang menjadi faktor pengali adalah 1, 2, 3, 4. Langkah selanjutnya adalah melakukan proses enkripsi triangle pertama:

1. Proses Enkripsi Triangle Pertama, untuk baris pertama (i = 1)

$M_{[11]} = P[1] + (K * R[1])\ mod\ 256 = \big(\boldsymbol{A} + (2 * R[1])\big) mod\ 256 = 67$ (huruf **C**)

$M_{[12]} = P[2] + (K * R[1])\ mod\ 256 = \big(\boldsymbol{F} + (2 * R[1])\big) mod\ 256 = 72$ (huruf **H**)

Lakukan hal yang sama sampai $M_{[44]}$ maka hasil dari enkripsi baris pertama (i = 1) yaitu:

Tabel 1. Hasil Enkripsi Triangle Pertama

Plaintext = AFAN								
Ciphertext				**Hasil enkripsi pada**		**M_{ij}**	**Nilai Karakter**	**Nilai Desimal**
				i	**j = (N+i) - N**			
C	H	C	O	1	(4+1) – 4 = 1	M_{11}	C	67
	L	G	S	2	(4+2) – 4 = 2	M_{22}	L	76
		M	Y	3	(4+3) – 4 = 3	M_{33}	M	77
			a	4	(4+4) – 4 = 4	M_{44}	a	97
Hasil enkripsi triangle pertama = CLMa								

2. Proses Enkripsi Triangle ke Dua, untuk baris pertama (i = 1)

$M_{[11]} = P[1] + (K * R[1])\ mod\ 256 = \big(\boldsymbol{C} + (2 * R[1])\big) mod\ 256 = 69$ (huruf **E**)

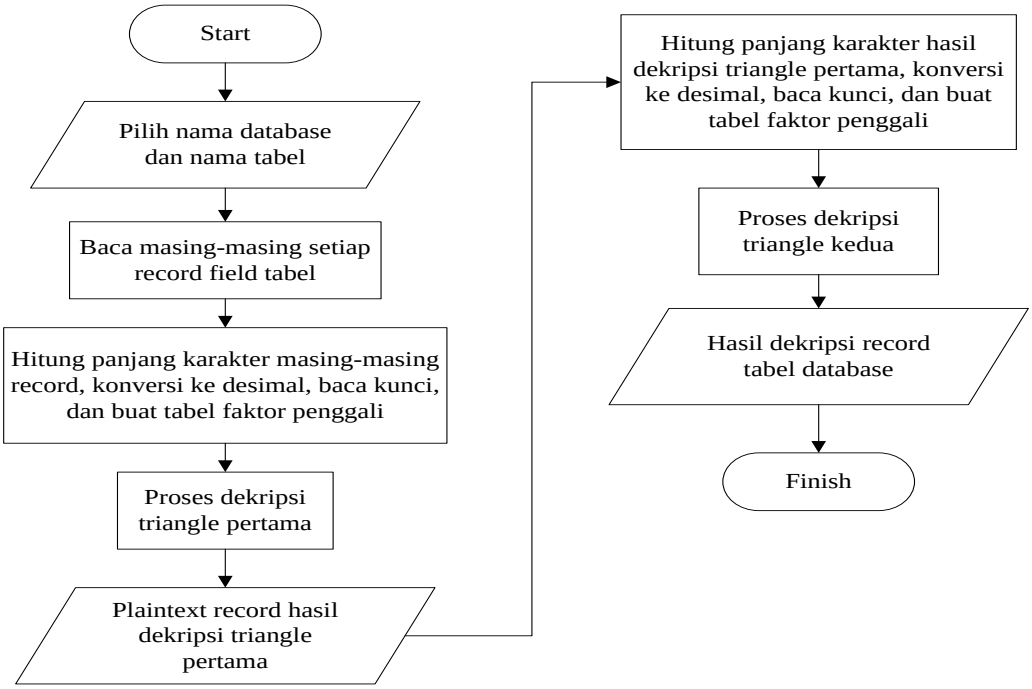
$M_{[12]} = P[2] + (K * R[1])\ mod\ 256 = \big(\boldsymbol{L} + (2 * R[1])\big) mod\ 256 = 78$ (huruf **N**)

Lakukan hal yang sama sampai $M_{[44]}$ maka hasil dari enkripsi baris kedua (i = 1) yaitu:

Tabel 2. Hasil Enkripsi Triangle Kedua

Plaintext = **CLMa**								
Ciphertext				**Hasil enkripsi pada**		**M_{ij}**	**Nilai Karakter**	**Nilai Desimal**
				i	**j = (N+i) - N**			
E	N	O	**c**	1	(4+1) – 4 = 1	M_{14}	c	99
I	R	**S**		2	(4+2) – 4 = 2	M_{23}	S	83
N	X			3	(4+3) – 4 = 3	M_{32}	X	88
W				4	(4+4) – 4 = 4	M_{41}	W	87
Hasil enkripsi triangle kedua = WXSc								

Proses dekripsi merupakan kebalikan dari proses enkripsi record database yang telah dilakukan sebelumnya. Kunci dan faktor pengali yang digunakan tetap sama seperti pada proses enkripsi. Proses dekripsi record database diawali pemilihan nama database kemudian memilih tabel yang telah dienkripsi. Semua record tabel yang telah dipilih akan dikembalikan ke teks record semula (*sebelum dienkripsi*). Adapun proses dekripsi record tabel database menggunakan algoritma Triangle Chain dapat dijelaskan dalam bentuk flowchart seperti terlihat pada gambar 5.



Gambar 5. Flowchart Dekripsi Record Database Algoritma Triangle Chain

Berdasarkan gambar 5 proses dekripsi dilakukan dengan dua tahap yaitu dekripsi triangle pertama dan dekripsi triangle kedua, sehingga dihasilkan plaintext akhir yang nantinya menjadi record database asli. Penyelesaian tahap dekripsi di atas dapat diuraikan melalui contoh kasus penyandian sebuah record di bawah ini:

Ciphertext	W	X	S	c
Nilai Desimal	87	88	83	99
Kunci	2 (*bilangan asli integer*)			

Jumlah deret bilangan akan disesuaikan dengan jumlah banyaknya karakter dari ciphertext. Jadi, jumlah karakter ciphertext (N) adalah 4. Deret bilangan asli (R) yang menjadi faktor pengali adalah 1, 2, 3, 4. Langkah selanjutnya adalah melakukan proses dekripsi triangle pertama:

1. Proses Dekripsi Triangle Pertama, untuk baris pertama (i = 1)

$M_{[11]} = C[1] - (K * R[1])\ mod\ 256 = \big(\boldsymbol{W} - (2 * R[1])\big) mod\ 256 = 85$ (huruf **U**)

$M_{[12]} = C[2] - (K * R[1])\ mod\ 256 = \big(\boldsymbol{X} - (2 * R[1])\big) mod\ 256 = 86$ (huruf **V**)

Lakukan hal yang sama sampai $M_{[44]}$ maka hasil dari dekripsi baris pertama (i = 1) yaitu:

Tabel 3. Hasil Dekripsi Triangle Pertama

Ciphertext = WXSc								
Ciphertext				**Hasil dekripsi pada**		**M_{ij}**	**Nilai Karakter**	**Nilai Desimal**
				i	**j = (N+i) - N**			
U	V	Q	**a**	1	(4+1) – 1 = 4	M_{14}	a	97
Q	R	**M**		2	(4+1) – 2 = 3	M_{23}	M	77
K	P			3	(4+1) – 3 = 2	M_{32}	P	80
C				4	(4+1) – 4 = 1	M_{41}	C	67
Hasil dekripsi triangle pertama = **CPMa**								

2. Proses Dekripsi Triangle Kedua, untuk baris pertama (i = 1)

$M_{[11]} = C[1] - (K * R[1])\ mod\ 256 = \big(\boldsymbol{C} - (2 * R[1])\big) mod\ 256 = 65$ (huruf **A**)

$M_{[12]} = C[2] - (K * R[1])\ mod\ 256 = \big(\boldsymbol{P} - (2 * R[1])\big) mod\ 256 = 78$ (huruf **N**)

Lakukan hal yang sama sampai $M_{[44]}$ maka hasil dari dekripsi baris pertama (i = 1) yaitu:

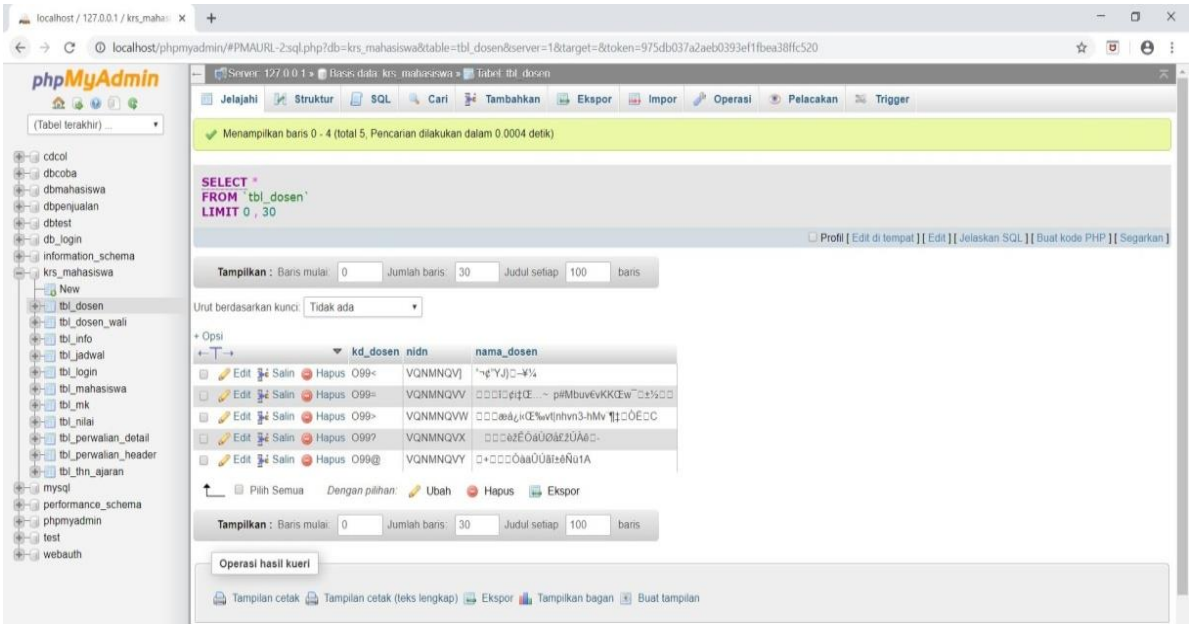
Tabel 4. Hasil Dekripsi Triangle Kedua

*Ciphertext*t = CPMa								
Ciphertext				**Hasil enkripsi pada**		**M_{ij}**	**Nilai Karakter**	**Nilai Desimal**
				i	**j = (N+i) - N**			
A	N	K	_	1	(4+1) – 4 = 1	M_{14}	A	65
	F	I	[	2	(4+2) – 4 = 2	M_{23}	F	70
		A	U	3	(4+3) – 4 = 3	M_{32}	A	65
			N	4	(4+4) – 4 = 4	M_{41}	N	78
Hasil dekripsi triangle ke dua = AFAN								

Plaintext yang dihasilkan pada proses dekripsi triangle ke dua adalah plaintext yang sebenarnya. Plaintext ini kemudian untuk menggantikan record tabel database yang telah tersandikan.

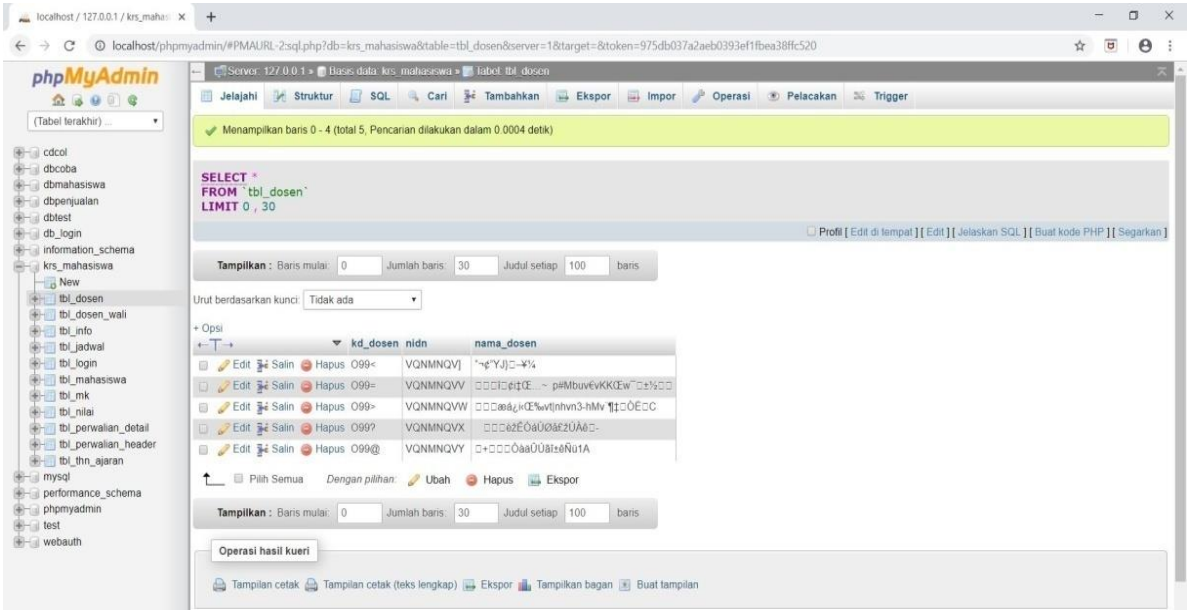
4. HASIL DAN PEMBAHASAN

Dalam penelitian ini model replikasi yang digunakan adalah replikasi data asynchronous dengan tambahan pengamanan dengan algoritma Triangle Chain. Untuk replikasi asynchronous pada basis data MySQL, yaitu dimana salah satu ada yang bertindak sebagai komputer master dan yang lain sebagai komputer slave, Untuk cara kerja replikasi nantinya apabila data yang di laptop master dirubah dan dienkripsi maka otomatis di laptop slave juga akan berubah serta record table database dalam keadaan terenkripsi, sehingga tingkat keamanan data lebih terjamin. Untuk menerapkan konsep replikasi database maka ada beberapa tahapan yang harus dilakukan sebelum akhirnya model replikasi database dapat berjalan. Diasumsikan untuk IP server-master adalah (192.168.1.1) sedangkan untuk server-slave adalah (192.168.1.2).



Gambar 6. Tampilan Hasil Enkripsi Database di Server Master

Setelah database dienkripsi maka sistem replikasi juga berjalan dengan mereplikasi perubahan database pada server master ke database server slave. Jika database pada server slave diakses dengan menggunakan phpMyAdmin maka hasilnya seperti terlihat pada gambar 7.



Gambar 7. Tampilan Hasil Enkripsi Database di Server Slave

Berdasarkan gambar 6 dan gambar 7 terlihat hasil enkripsi database di server master berhasil direplikasi ke database server slave. Hal ini dibuktikan dengan melihat isi database pada master sama persis dengan isi database pada slave, maka dapat disimpulkan proses enkripsi replikasi database model asynchronous dengan pengamanan enkripsi algoritma Triangle Chain berhasil di ujicobakan pada jaringan LAN.

5. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan sebelumnya, maka ditarik kesimpulan bahwa penerapan model replikasi asynchronous pada database MySQL yang terdiri dari satu master server dan satu slave server dan saling terhubung dalam jaringan host-to-host dengan menggunakan kabel UTP maka setiap perubahan data yang terjadi secara berkala akan selalu melakukan sinkronisasi atau backup data pada komputer slave sehingga jika terjadi kegagalan dalam sistem, masih tetap memiliki salinan pada server utama yang akan menjaga ketersediaan data tetap valid dan konsisten.

Penerapan replikasi database dalam penelitian ini dikombinasikan dengan algoritma kriptografi Triangle Chain, dari hasil pengujian sistem menunjukkan bahwa algoritma Triangle Chain dapat meningkatkan keamanan pada replikasi database, karena setiap record data pada tabel database akan terlebih dahulu dienkripsi sebelum direplikasi ke database slave sehingga dapat melindungi dari gangguan maupun serangan dari pihak yang tidak bertanggung jawab.

REFERENSI

[1] P. L. L. Belluano, "Penerapan Sistem Replikasi dan Integrasi Basis DataTerdistribusi Pada Pangkalan Data Pendidikan Tinggi (*PDPT*)," *Ilk. J. Ilm.*, vol. 9, no. 1, pp. 42–48, 2017, [*Online*]. Available: Poe3.setiawan@gmail.com

[2] D. Muh Hidayat, Isnawaty, and Subardin, "Perancangan dan Implementasi Sistem Replikasi Database Terdistribusi pada Fakultas Teknik Universitas Halu Oleo," *semanTIK*, vol. 4, no. 2, pp. 91–98, 2018.

[3] S. A. Pebresega and D. Kusumaningsih, "Implementasi Algoritma Kriptografi Triangle Chain Cipher (*TCC*) untuk Pengamanan Database Berbasis Desktop pada CV.Usaha Tani," *Skanika*, vol. 1, no. 1, pp. 380–384, 2018.

[4] Mashuri, "Implementasi Sistem Database Terdistribusi dengan Metode Partial Replication," *J. Inf. Technol. Comput. Sci.*, vol. 3, no. 2, 2020.

[5] A. Heryanto and Albert, "Implementasi Sistem Database Terdistribusi Dengan Metode Multi-Master Database Replication," *J. MEDIA Inform. BUDIDARMA*, vol. 3, no. 1, pp. 30–36, 2019, doi: 10.30865/mib.v3i1.1098.

[6] H. Maulana, "Analisis Dan Perancangan Sistem Replikasi Database MySQL Dengan Menggunakan Vmware Pada Sistem Operasi Open Source," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 32–37, 2016.

[7] R. K. Hondro, "ANALISIS DAN PERANCANGAN SISTEM YANG MENERAPKAN ALGORITMA TRIANGLE CHAIN CIPHER (*TCC*) UNTUK ENKRIPSI RECORD TABEL DATABASE," *J. Teknol. Inf. dan Komun.*, vol. 3, no. 2, 2014.

[8] Y. Irawan, "Implementasi Algoritma Triangle Chain Cipher dalam Penyandian Pesan," *KAKIFIKOM (Kumpulan Artik. Karya Ilm. Fak. Ilmu Komput.*, vol. 02, no. 02, pp. 83–92, 2020.

[9] V. I. Anggraini, "IMPLEMENTASI ALGORITMA TRIANGLE CHAIN CIPHER DAN GOST PADA PENGAMANAN CITRA DIGITAL," *Bull. Inf. Technol. (BIT)*, vol. 2, no. 3, pp. 118–128, 2021.

[10] T. Zebua, "Analisa dan Implementasi Algoritma Triangle Chain pada Penyandian Record Database," *Pelita Inform. Budi Darma*, vol. 3, no. 2, pp. 37–49, 2013.