Implementasi Pengamanan Data Koperasi Menggunakan Algoritma *Advanced Encryption Standard* (Aes)

Mohammad Imron[1] , Ilham Ardiansyah[2], Didit Suhartono[3]
[123]Teknik Informatika, STMIK AMIKOM Purwokerto, Indonesia
Email : imron@amikompurwokerto.ac.id[1], kaykha16@gmail.com[2], didit@amikompurwokerto.ac.id[3]

***Abstrak*—Koperasi NASARI Purwokerto telah menerapkan teknologi informasi untuk pengolahan data dengan meningkatkan pertumbuhan ekonomi dalam segala bidang, sehingga sudah sewajarnya jika setiap sektor mengalami perkembangan. Demikian juga dengan sektor koperasi yang perannya masih sangat dibutuhkan untuk menunjang perekonomian masyarakat Indonesia yang sebagian besar terdiri dari golongan menengah kebawah. Akan tetapi data-data yang tersimpan di koperasi NASARI Purwokerto masih berupa data asli yang belum terenkripsi,dari perkembangan tersebut terdapat dampak negatif berupa pengambil alihan data, pemanipulasian data atau terjadinya penyadapan data.Kriptografi merupakan salah satu cara atau metode dalam pengamanan data yang tepat untuk menjaga kerahasiaan dan keaslian data, sehingga dapat meningkatkan aspek keamanan suatu data yang ada dikoperasi. Penelitian ini menggunakan algoritma AES (*Advanced Encryption standard*), yang diharapkan dari penelitian ini adalah membangun sistem keamanan data koperasi dengan sistem enkripsi AES. Dan penelitian ini peneliti menggunakan standar *Rijndel Managed* yang merupakan standar kriptografi yang terdiri dari 3 blok cipher, yaitu AES-128, AES-192, AES-256. Dari hasil penelitian yang dilakukan peneliti bahwa algoritma AES dengan panjang 256 bit berupa aplikasi desktop yang berfungsi untuk mengamankan data koperasi, yang telah diimplementasikan sangat berguna untuk mengamankan data dan tingkat kesulitan untuk memecahkan hasil enkripsinya sulit dan hasil kriptografi AES tersebut menghasilkan cipher 16 bit.**

Kunci —Kriptografi, *Advanced Encryption Standard*, Aplikasi Desktop, Data Koperasi.

I. PENDAHULUAN

Sejalan dengan meningkatnya pertumbuhan ekonomi dalam segala bidang, sehingga sudah sewajarnya jika setiap sektor mengalami perkembangan. Demikian juga dengan sektor koperasi yang perannya masih sangat dibutuhkan untuk menunjang perekonomian masyarakat Indonesia yang sebagian besar terdiri dari golongan menengah kebawah.

Penggunaan komputer dalam berbagai bidang memberikan dampak perkembangan yang sangat pesat pada sebuah perangkat keras ataupun perangkat lunak, dimana sebuah kelompok atau organisasi membutuhkan adany.a komputerisasi dalam setiap kegiatannya. Sehingga dari hal tersebut penggunaan komputerisasi membutuhkan sebuah keamanan data agar aset-aset tidak disalah gunakan oleh pihak yang tidak bertanggung jawab begitu juga dengan data yang ada di koperasi NASARI Purwokerto.

Penelitian yang telah dilakukan Andreanus, dkk [1] tentang Sistem Pengamanan Data Menggunakan Metode MD5 dan *Private Key* pada Aplikasi Berbasis *Client Server* di Koperasi Buah Hati Bawen pada sebuah basis data untuk mengenkripsi sistem pengamanan pada jaringan *client server* pada *password* yang akan dikirim *client* ke *server*. Sehingga dapat ditarik kesimpulan bahwa informasi dan data-data penting perusahaan menjadi hal yang sensitif apabila data menyangkut perusahaan privasi yang tidak boleh orang lain tahu, maka demi menjaga kerahasian informasi data tersebut diperlukan sistem pengamanan data dari berbagai ancaman yang mungkin timbul.

Dalam hal ini perlindungan data dapat dilakukan dengan menggunakan sebuah algoritma keamanan data yang sering digunakan adalah kriptografi, algoritma ini dapat melakukan sebuah pengamanan pada file atau data yang akan dilindungi.

Kerahasiaan informasi dapat diperoleh memlalui proses enkripsi dan dekripsi. Proses enkripsi sendiri mengubah pesan asli menjadi pesan yang tidak dapat dibaca atau pesan yang tersandi, sedangkan dekripsi mengembalikan data yang tersandi menjadi bentuk data asli.

Pada penelitian ini peneliti menggunakan algoritma AES (*Advanced Encryption Standard*), yang diharapkan dari penelitian ini adalah untuk membangun sistem keamanan data koperasi dengan sistem enkripsi AES. Algoritma AES dipilih peneliti, dikarenakan AES merupakan *cipher* yang berorientasi pada bit, sehingga memungkinkan untuk implementasi algoritma yang efisien kedalam perangkat lunak dan perangkat keras. AES sendiri memiliki ketahanan terhadap semua jenis serangan yang diketahui.

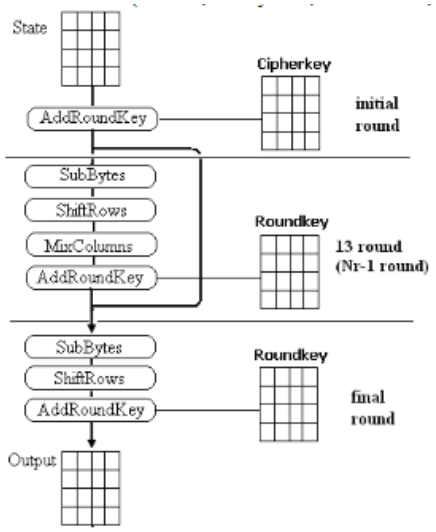
II. METODE ADVANCED ENCRYPTION STANDARD (AES)

Pada metode ini diterpakan pada rancangan program kriptografi implementasi *Advanced Encryption Standard*, dimana program ini dirancang untuk dapat mengenkripsikan dan mendekripsikan data di koperasi NASARI Purwokerto. Dan yang menjadi masukkan program tersebut adalah data

digital, sedangkan keluaran dari data tersebut berupa enkripsi/dekripsi.

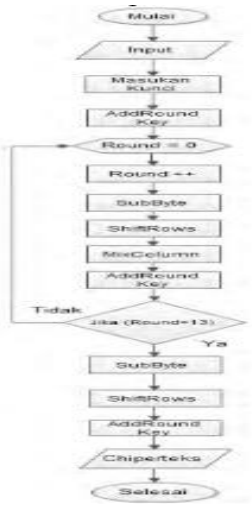
A. *Proses Enkripsi AES*

Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumn, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dicopykan ke dalam state akan mengalami transformasi byte AddRaoundKey. Setelah itu, state akan mengalami transformasi SubBytes, shiftRows, MixColumns, dan AddRaoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai round function. Raound yang terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumn[2].



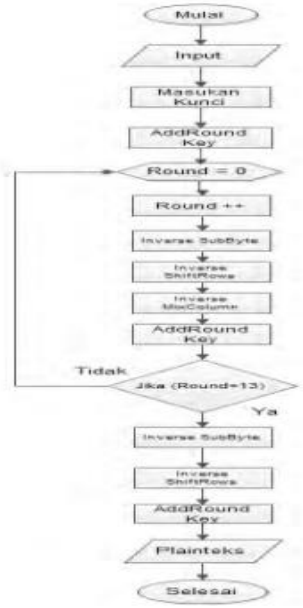
Gambar 1. Proses Enkripsi [2]

B. *Proses Enkripsi dan Dekripsi Metode Advanced Encryption Standard (AES)*



Gambar 2. Proses Enkripsi Algoritma AES

Pada proses enkripsi diatas menjelaskan proses menggunakan algoritma kriptografi AES. Pada langkah awal dalam melakukan proses enkripsi sebuah data harus melakukan input data yang akan dienkripsi.



Gambar 3. Proses Dekripsi Algoritma AES

Pada gambar diatas menjelaskan proses dekripsi menggunakan algoritma kriptografi AES, dimana langkah proses dekripsi harus melakukan input dari hasil cipherteks yang akan didekripsi.

III. HASIL DAN PEMBAHASAN

Berdasarkan hasil penelitian yang telah dilakukan, maka telah didapatkan hasil implementasi pengamanan data koperasi menggunakan metode *Advanced Encryption standard* (AES), dimana penelitian ini peneliti mengimplementasikan kriptografi AES dengan menggunakan bahasa C# dan aplikasi yang digunakan Visual Studio 2012, dikarenakan didalam aplikasi tersebut sudah terdapat *function / library* untuk kriptografi.

```
clsCrypto
using System;
using System.Security.Cryptography;
```

Gambar 4. *Library* untuk Kriptografi.

Dimana source code diatas digunakan untuk memanggil library yang berfungsi untuk keamanan kriptografi.

Setelah dilakukan pembuatan aplikasi, maka pada bagian ini penulis akan menguraikan proses yang terjadi pada sistem pengamanan data koperasi. Dengan melalui sistem ini diharapkan dapat memberikan kontribusi untuk mengamankan data terutama dalam mengolah data-data yang bersangkutan dengan sistem koperasi.

Pada metode enkripsi dan dekripsi penelitian ini menggunakan standar Rijndeal Managed yang merupakan standar kriptografi yang terdiri dari 3 block cipher, yaitu AES-128, AES-192, dan AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Sehingga memudahkan dalam algoritma enkripsinya, berikut source code enkripsi dan dekripsi;

1) Source Code Enkripsi

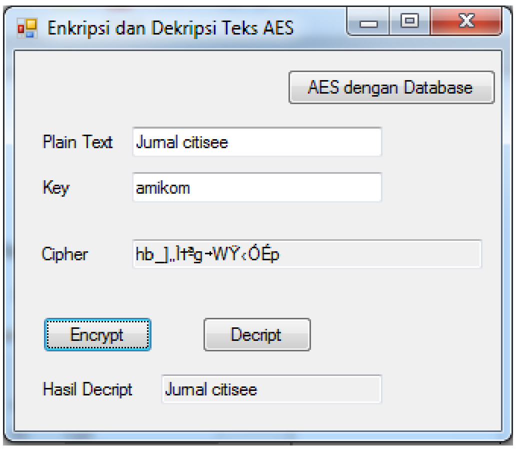
```
//Untuk meng-encrypt data menggunakan encrypt AES
protected internal string Encrypt(string strInput, CipherMode cipherMode)
{
    string strOutput = string.Empty;
    if (!string.IsNullOrEmpty(strInput))
    {
        try
        {
            byte[] bytePlainText = Encoding.Default.GetBytes(strInput);
            using (RijndaelManaged rijManaged = new RijndaelManaged())
            {
                rijManaged.Mode = cipherMode;
                rijManaged.BlockSize = 128;
                rijManaged.KeySize = 128;
                rijManaged.IV = GenerateIV();
                rijManaged.Key = GenerateKey();
                rijManaged.Padding = PaddingMode.Zeros;
                ICryptoTransform icpoTransform = rijManaged.CreateEncryptor(rijManaged.Key, rijManaged.IV);
                using (MemoryStream memStream = new MemoryStream())
                {
                    using (CryptoStream cpoStream = new CryptoStream(memStream, icpoTransform, CryptoStreamMode.Write))
                    {
                        cpoStream.Write(bytePlainText, 0, bytePlainText.Length);
                        cpoStream.FlushFinalBlock();
                    }
                    strOutput = Encoding.Default.GetString(memStream.ToArray());
                }
            }
        }
        catch (Exception ex)
        {
            MessageBox.Show(ex.Message);
        }
    }
```

2) Source Code Dekripsi

```
//Untuk men-dencrypt data menggunakan encrypt AES
protected internal string Decrypt(string strInput, CipherMode cipherMode)
{
    string strOutput = string.Empty;
    if (!string.IsNullOrEmpty(strInput))
    {
        try
        {
            byte[] byteCipherText = Encoding.Default.GetBytes(strInput);
            byte[] byteBuffer = new byte[strInput.Length];
            using (RijndaelManaged rijManaged = new RijndaelManaged())
            {
                rijManaged.Mode = cipherMode;
                rijManaged.BlockSize = 128;
                rijManaged.KeySize = 128;
                rijManaged.IV = GenerateIV();
                rijManaged.Key = GenerateKey();
                rijManaged.Padding = PaddingMode.Zeros;
                ICryptoTransform icpoTransform = rijManaged.CreateDecryptor(rijManaged.Key, rijManaged.IV);
                using (MemoryStream memStream = new MemoryStream(byteCipherText))
                {
                    using (CryptoStream cpoStream = new CryptoStream(memStream, icpoTransform, CryptoStreamMode.Read))
                    {
                        cpoStream.Read(byteBuffer, 0, byteBuffer.Length);
                    }
                    strOutput = Encoding.Default.GetString(byteBuffer);
                }
            }
        }
        catch (Exception ex)
        {
            MessageBox.Show(ex.Message);
        }
    }
```

A. Proses Enkripsi pada Data Koperasi

Berikut adalah antar muka berupa form yang dibangun untuk mempermudah pengguna berinteraksi dengan sistem, berikut tampilan awal.



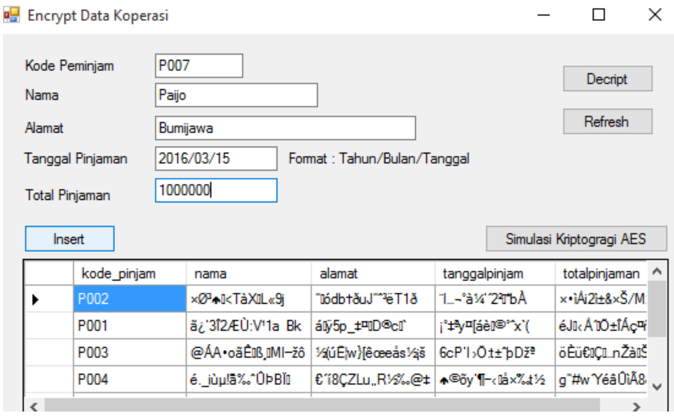
Gambar 5. Antar muka Enkripsi dan Dekripsi

Berikut akan dilakukan proses pengujian pada data koperasi dengan menerapkan kriptografi AES yaitu proses enkripsi pada saat input data, sehingga data yang masuk pada data merupakan data enkripsi (*cipher*). Kemudian data plaintex akan dipisahkan pada table yang berbeda, berikut source code insert data;

```
private void btninsert_Click(object sender, EventArgs e)
{
    aes.IV = "tugas";
    aes.KEY = "kripto";
        Conn.Open();
        MySqlCommand cmd = new MySqlCommand();
        cmd.Connection = Conn;
        cmd.CommandType = CommandType.Text;
        String nama = aes.Encrypt(txtnama.Text, CipherMode.CBC);
        String alamat = aes.Encrypt(txtalamat.Text, CipherMode.CBC);
        String tanggal = aes.Encrypt(txttanggal.Text, CipherMode.CBC);
        String pinjam = aes.Encrypt(txtpinjaman.Text, CipherMode.CBC);
        cmd.CommandText = "insert into log values('" + txtkode.Text + "','" + nama + "','" + alamat + "','"
            + tanggal + "','" + pinjam + "')";
        cmd.ExecuteNonQuery();
        cmd.CommandText = "insert into pinjaman values('" + txtkode.Text + "','" + txtnama.Text + "','"
                + txtalamat.Text + "','" + txttanggal.Text + "','" + int.Parse(txtpinjaman.Text) + "')";
        cmd.ExecuteNonQuery();

        Conn.Close();
        showdata();
        txtkode.Text = "";
        txtnama.Text = "";
        txtalamat.Text = "";
        txttanggal.Text = "";
        txtpinjaman.Text = "";
}
```

Sehingga hasil proses enkripsi input data pada data koperasi seperti pada gambar 5.



Gambar6. Proses enkripsi data koperasi.

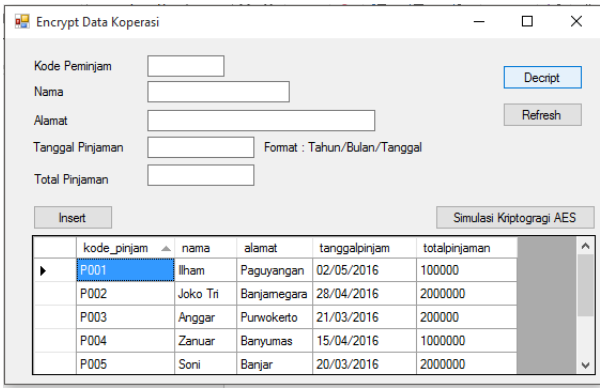
Pada proses data peminjam dengan nama "Paijo" yang tersimpan pada data berubah menjadi cipher, sehingga tidak dapat dibaca.

kode_pinjam	nama	alamat	tanggalpinjam	totalpinjaman
P002	×Ø³<TàXL«9 j	"ódb†ðuJ"˜³ëT1ð	¨l…¬°à¼'´2²*bÀ	×•ìÅi2ì±&× Š/M>î
P001	ã¿'3Î2ÆÙ:V'1aBk	áÿ5p_‡¤D ®c`	¡°‡ªy¤[áè©°ˆx`(	éJ‹Å´Ö±ÎÁç¤ñL
P003	@ÁA•oãÊß¸MI—žô	½(úË¦w}[êœeås½¡š	6cP'l›Ö:t±ˆþDžª	öÈü€Ç…nŽàŠù—
P004	é._iùµ!˜â‰ˆÛÞBÏ	€´í8ÇZLu„R½‰@‡	©õy'¶–‹å×˜‰t½	g"#w´YéâÛìÃ8ð„=
P005	ãŠÂxz7Ížh_]§¼	¦‰›KJ}¢#É÷naÁ	ËV_ÌP9¥Úœ)>¢6	×•ìÅi2ì±&× Š/M>î
P010	½)(Sªtè‰ºh-Æe/p	±È~Ú—/È"÷—	vÿóØêV"+J¡ sÖ	öÈü€Ç…nŽàŠù—
P007	XþÈqõZ»aùM0BÒ	820„µ—DÙð}ÞM§	†/:˜lþtÿ7Áà¨	g"#w´YéâÛìÃ8ð„=

Gambar 7. Hasil enkripsi data koperasi.

B. Proses Dekripsi pada data Koperasi

Sedang proses untuk mengembalikan hasil enkripsi data dilakukan dengan cara memanggil hasil proses yang telah berubah menjadi cipher. Dimana databse yang terdekripsi dengan kunci yang cocok tersebut dapat kembali seperti data sebelumnya, terlihat pada gambar 8.



Gambar 8. Proses Hasil Dekripsi

IV. KESIMPULAN

Dari hasil hasil pengamanan Data menggunakan Metode MD5 berbasis *client server* di koperasi buah hati Bawen [1] implementasi aplikasi sistem tersebut didapat, bahwa program dapat berjalan dengan baik dalam mengenkripsi dan mendekripsikan kembali data yang berbasi *client server* tersebut hanya mengimplementasikan pada pemberian no PIN, dari pengujian peneliti banyaknya kunci yang digunakan dapat menambah kesulitan bagi kriptanalis sehingga merepotkan. Algoritma AES jumlah panjang 256 bit dapat mengamankan data koperasi dengan menghasilkan cipher 16 bit.

Dengan adanya sistem yang dibangun ini dapat memberikan keamanan terhadap data koperasi, sehingga data dapat terlindungi dengan aman.

REFERENCES

[1] Dody, dkk, (2011). Sistem Pengamanan Data menggunakan Metode MD5 dan *Private Key* pada Aplikasi Berbasis *Client Server*,Jurnal Teknologi Informasi-Aiti, Vol 8. No.2, Agustus :101-202.
[2] Yuniat, V. i., Indriyanta, G., & Rachmat, A. (2009). Enkripsi Dan Dekripsi Dengan Algoritma AES 256 Untuk Semua Jenis File. Jurnal Informatika Volume 5.
[4] Yusuf Kurniawan, Kriptografi Keamanan Internet dan Jaringan Komunikasi. Bandung: Informatika Bandung, 2004.
[5] Wihartantyo Ari Wibowo, ADVANCED ENCRYPTION STANDARD, ALGORITMA RIJNDAEL. Bandung: Departemen Teknik Elektro ITB, 2004.
[6]Dony Ariyus, Kriptografi Keamanan Data dan Komunikasi. Yogyakarta: Andi Offset, 2005.
[7] Munkner, H. (1987), Hukum Koperasi, Bandung, Penerbit Alumni.
[8] Simarmata, Janner & Paryudi, Imam. (2006),Basis Data, Andi Offset, Yogyakarta.