**IMPLEMENTASI ALGORITMA *ADVANCE ENCRYPTION STANDARD* (AES) 128 DAN QR – CODE PADA APLIKASI E – HALAL BERBASIS ANDROID, PHP DAN MYSQL**

**Dede Husen**

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Kuningan

*E-mail :dede.husen@student.uniku.ac.id*

**ABSTRAK**

Indonesia adalah negara dengan mayoritas penduduk muslim terbanyak didunia, mengkonsumsi makanan halal adalah suatu kewajiban bagi konsumen muslim, salah satu metode yang dilakukan oleh pemerintah adalah dengan pemberian no sertifikasi pada makanan melalui LPPOM MUI yang nanti pada tahun 2019 akan berpindah melalui lembaga resmi Badan Penyelenggara Jaminan Produk Halal, maka dari itu diperlukan sebuah aplikasi yang dapat memeriksa langsung keaslian nomor sertifikasi tersebut berdasarkan database dari lembaga terkait. Dengan menggunakan teknologi QR – Code dan algoritma kriptografi *Advance Encryption Standard* (AES) 128 yang di tanam pada aplikasi android ini menajdikan data yang terkandung pada pada nomor sertifikasi akan aman dan sangat sulit untuk di palsukan dan semua proses enkripsi dan deskripsi data dilakukan di server (Web). Aplikasi ini dikembangkan dengan menggunakan metode *Rational Unified Process* (RUP) dimana tahapan – tahapan akan lebih jelas dan terstruktur dengan baik. Hasil dari penelitian ini adalah sebuah aplikasi berbasis client server dimana pada client adalah sebuah aplikasi android dengan fitur utama scan QR – Code khusus yang berfungsi untuk melakukan scanning Qr code pada produk dan dari sisi server sebagai antarmuka dalam memanajemen data sertifikasi baik itu generate Qr code dan proses enskripsi atau deskripsi data.

**Kata kunci** : sertifikasi halal, android, *Advance Encryption Standard*, Qr – Code, *Rational Unified Process*

*Indonesia is a country with the majority of the world's largest Muslim population. Consuming halal food is an obligation for Muslim. One of methods undertaken by the government is granting certification number on food through LPPOM MUI which later in 2019 will move through the Halal Product Assurance Agency, therefore it required an application that can check the authenticity of the certification number based on the database of the relevant agencies. Using the QR - Code technology and the Advance Encryption Standard (AES) 128 cryptographic algorithm embedded in this android application, the data contained in the certification number will be safe and it is very difficult to fake and all encryption processes and data descriptions are performed on the server (Web). This application was developed using the Rational Unified Process (RUP) method in which the stages will be clearer and well structured. The result of this research is that a client server based application where the client is an android application with the main feature of special QR - Code scan that serves to perform the scanning Qr code on the product and from the server side is the interface in managing of certification data whether it generates Qr code and encryption process or data description.*

***Keyword*** *: Halal Certification, Android, Advance Encryption Standard, Qr- Code, Rational Unified Process.*

1. **PENDAHULUAN**

Dalam kegiatan produksi dan perdagangan produk pangan di era globalisasi ini, masyarakat yang mengkonsumsi, khususnya umat islam perlu diberikan pengetahuan tentang kehalalan produk, informasi dan akses yang memadai agar memperoleh informasi yang benar tentang status kehalalan produk yang dibelinya, terlebih semakin ban,yaknya produk – produk asing yang masuk ke tanah air yang kehalalanya tentunya akan sangat sulit diketahui. Maka dari itu pemerintah saat ini dengan berdasarkan UU No 33 tahun 2014 (UU JPH) tentang jaminan produk. halal melalui Kementrian Agama membentuk Badan Penyelenggara Jaminan Produk Halal (BPJPH) yang telah diresmikan pada tanggal 10 november 2017 yang tentunya akan menjadi lembaga yang mengelola sertifikasi kehalalan sebuah produk baik itu makanan, minuman, kosmetik dan obat – obatan dengan masa berlaku selama 2 tahun yang kemudian bisa di perpanjang kembali, dan pada awalnya semua proses tersebut yang sebelumnya oleh dikelola oleh Lembaga Pengkajian Pangan, Obat-obatan, dan Kosmetika Majelis Ulama Indonesia ( **LPPOM MUI ).**

Maka dari permasalahan itu perlu adanya pengembangan dari sistem yang ada dan penambahan *platform* baru atau sebuah media dimana kita sebagai konsumen dapat mengecek langsung ke aslian data sertifikasi kehalalan produk tersebut dengan praktis, mudah, *real* *time* dan terpercaya berdasarkan data dari lembaga terkait. Dan berdasarkan beberapa hal tersebut akan menjadikan dasar sebagai bahan penelitian tugas akhir saya.

Dengan memanfaatkan teknologi *Quick Response Code* (QR Code) yang di kombinasikan dengan algoritma Kriptografi *Advance Encryption Standard* (AES)128 yang di kembangkan dalam aplikasi android, cara kerjanya cukup sederhana yakni dengan menempelkan QR Code pada produk tersebut, dimana QR Code tersebut mengadung informasi yang dienkripsi oleh alogritma AES 128, dimana algoritma tersebut akan diterapkan pada QR Code tersebut kemudian kita dapat melakukan Pengecekan secara *Realtime* dengan melakukan *scanning* dengan aplikasi android yang kemudian aplikasi akan melakukan pemindaian dan kemudian mendeskripsikan data tersebut, setelah itu akan melakukan *checking* ke server apakah data yang ada pada QR Code tersebut valid atau tidak, kemudian aplikasi akan memberitahu apakah produk tersebut sudah tersertifikasi halal atau belum, dengan aplikasi tersebut tetntunya akan ada beberapa elemen – elemen yang terbantu, baik itu dari konsumen ataupun dari produsen.

1. METODE
2. Metode Penelitian

Metode penelitian yang di pakai pada pengembangan aplikasi ini adalah dengan menggunakan metode *Rational Unified Process* (RUP), metode ini penulis gunakan dikarnanakan dikarnakan konsep *object oriented* yang cocok dengan konsep aplikasi yang akan dibangun, berikut 4 fase tahapan :

1. *Inception*

Pada tahap ini lebih memodelkan proses bisnis yang di butuhkan (*business modelling*) dan mendifinisikan kebutuhan sistem yang akan dibuat (*requirements*). Dan pada tahap ini penulis melakukan perancangan use case bussines yang menggambarkan interkasi antara sistem atau aplikasi e-halal dengan user, selain itu penulis juga mengggambarkan *requirement workflow* yang menggambarkan sistem apa yang dilakukan dalam bentuk *use case diagram*  aplikasi E-halal.

1. *Elaboration* (perluasan dan perencanaan)

Tahap untuk melakukan desain secara lengkap berdasarkan hasil analisis ditahap *inception.* Aktivitas yang dilakukan pada tahap ini antara lain mencakup pembuatan desain arsitektur subsistem (*architecture pattern*), desain komponen sistem, desain format data (protokol komunikasi), desain antarmuka/tampilan, desain peta aliran tampilan, penentuan *design pattern* yang digunakan, pemodelan diagram UML (diagram *activity, class*) dan pembuatan dokumentasi.

Pada tahap ini penulis melakukan perancangan *user interface*, *database*, denagn mengguanakan sebuah dokumen yaitu spesisfikasi kebutuhan perangkat lunak (SKPL). Kedepanya apliksi e-halal ini akan di gunakan dalam masysarakat umum untuk melakukan pengecekan kehalalan suatu produk berdasakan nomor sertifikasi yang terdaftar di BPJH.

1. *Construction* (Konstruksi)

Tahap ini focus pada pengembangan komponen dan fitur – fitur sistem, implentasi kode – kode program dan pengujian peragkat lunak. Pada tahap ini penulis mulai melakukan penulisan kode – kode program (*coding)* degan menggunakan Bahasa pemrograman java untuk android (c*lient*), PHP untuk sisi web(server) dan MySQL untuk Pembuatan basis data.

1. *Transition*

Pada tahap ini penulis mulai menyerahkan sistem/aplikasi ke konsumen (*roll-out*), dilakuakan pelatihan, pemeliharaan, dan pengujian hasil akhir sisem, apakah sudah memenuhi kebutuhan user atau belum.

Akhir darike empat fase ini adalah produk perangkat lunak yang sudah lengkap. Keempat fase RUP ini dilakukan secara berurutan dan iterative dimana setiap interasi dapat digunakan untuk memperbaiki iterasi berikutya.

1. Analisis Kebutuhan

Analisis ini meliputi analisis kebutuhan fungsional dan non fungsional yang disusulkan dapat sesuai dengan kebutuhan dan dapat menyelesaikan permasalahan yang ada berdasarkan hasil pengamatan.

1. Analisis Kebutuhan Perangkat Keras antara lain :

* Laptop dengan spesifikasi
* Processor : Intel(R) Core(TM) i5-3337U CPU @ 1.80GHz (4 CPUs)
* RAM : 6 GB
* OS : Windows 10 Pro
* Hardisk : 500 GB
* Vga Card : NVIDIA GeForce 710 M
* Smartphone
* OS : Android Jelly Bean
* API Level : 17
* Kamera : 2 Mp
* Ram : 512 Mb
* Memori : 1 Gb

1. Kebutuhan Perangkat lunak

* Microsoft Windows 10 Pro
* Xampp V 3.2.2
* Android Studio V 3.1
* Notepad ++
* Browser Opera

1. HASIL DAN PEMBAHASAN
2. Desain Sistem
3. Usecase Diagram Aplikasi E-Halal



Gambar 3.1 Use Case Diagram Aplikasi E-Halal

Pada usecase terdapat 6 usecase utama antara lain Login admin, mengecek data halal, operasi algoritma, mengelola data halal, mengelola data user dan logout admin.

1. Sequence Diagram

Gambar 3.2 Sequence Diagram Cek data halal

1. Peracangan Database

Terdapat 2 tabel utama pada aplikasi ini antara lain tabel admin dan tabel data sertifikasi

* Tabel 3.1 Tabel Admin

|  |  |  |
| --- | --- | --- |
| Nama Field | Type | Length |
| id\_admin | Varchar | 10 |
| nama\_user | Varchar | 30 |
| Password | Varchar | 50 |
| Email | Varchar | 50 |

* Tabel 3.2 Tabel data sertifikasi

|  |  |  |
| --- | --- | --- |
| Nama Field | Type | Length |
| no\_sertifikat | varchar | 15 |
| nama\_produk | Varchar | 30 |
| nama\_perusahaan | Varchar | 50 |
| tgl\_buat | Date | 11 |
| exp\_date | date | 11 |

1. Implementasi Algoritma *Advance Encryption Standard* 128

Algoritm AES 128 adalah salah satu algoritma kriptografi dimana pada proses enskripsinya terdapat 4 langkah utama antara lain proses *SubBytes, ShiftRows, MixColumns dan AddRoudKey* dan Proses deskripsinya adalah kebalikan atau invers dari proses enkripsi antara lain *InvSubBytes, InvShifRows,InvMixColums* dan pada proses deskripsi ini addround key tidak di lakukan. Berikut implementasi

1. Enskripsi

Pada proses enskripsi algoritma AES 128 di sisipkan pada field no sertifkat yang diproses pada saat penginputan data yang hasil enskripsi tadi akan berbentuk *chipper text*  dan akan di generate ke dalam kedalam QR Code, berikut perbedaan antara Qr Code Standar dan Qr Code yang terenskripsi



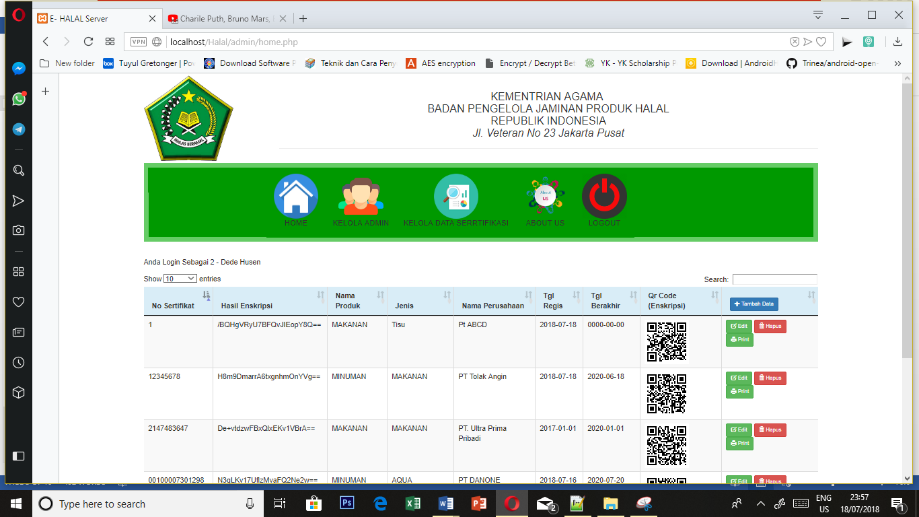
3.2 Generate Qr Code Standar

3.3 Generate Qr Code yang Terenkripsi

1. Deskripsi AES 128

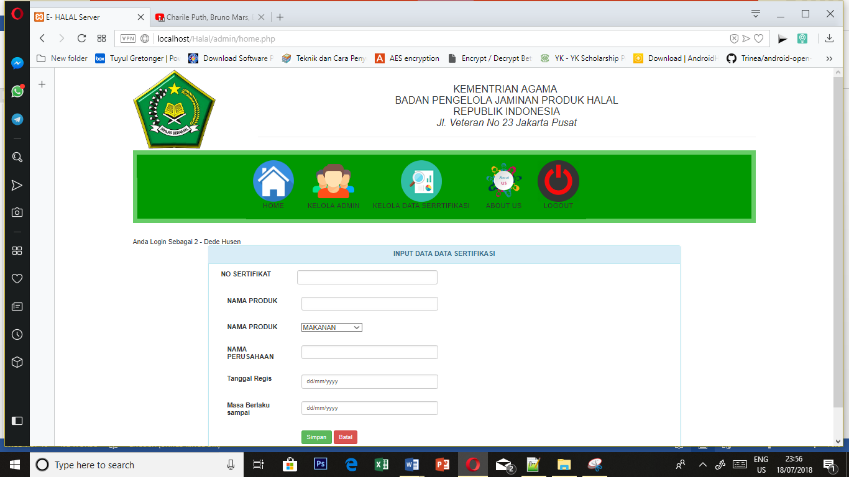
Pada proses deskripsi ini proses dilakukan di server saat hasil scanning qr code yang terenskripsi di kirim oleh aplikasi ke server dan di server akan dilakukan proses deskripsi yang kemudian jika hasil deskripsi teresebut valid maka akan di lakukan eksekusi quri berdasarkan data hasil enskripsi yang kemudian akan menampilkan data detail berdasarkan no sertifikat.

1. Interface Desain antarmuka

* Menu Tampil data Halal (server)

Gambar 3.4 Interface Pengelolaan data halal

Pada gambar diatas terdapat berberapa *field* yang berfungsi untuk menampung data setifikasi halal yang disimpan dalam database. terdapat beberapa tombol juga yang berfungsi untuk proses update data, print sertifikat, hapus data dan penambahan data

* Menu input data

Gambar 3.5 interface Input Data Halal

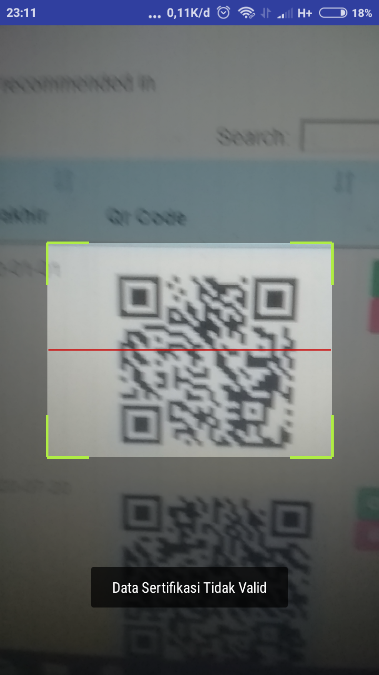
Interface aplikasi diatas berfungsi saat proses input data sertifiksi, dimana pada proses ini algoritma di sisipkan.

* Menu Utama (Aplikasi)



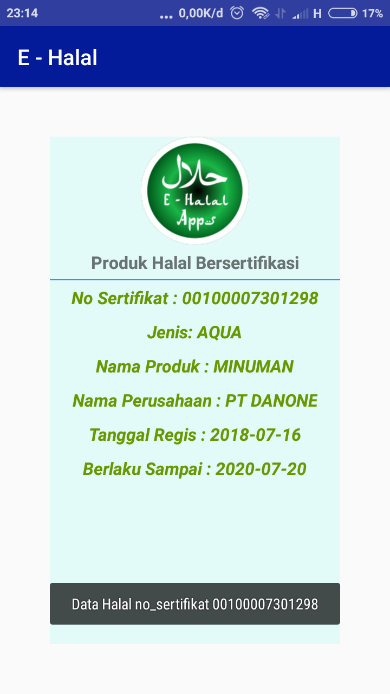
Gambar 3.6 Menu Utama

Gambar diatas menunjukan halam menu utama dimana terdapat 4 buah menu daintaranya menu Scan usntuk melakukan Scanning Qr Code, Input manual adalah melakukan pencarian manual, tombol news untuk berita dan tombol about us berisi tentang informasi pengembang.

* Proses Scanning

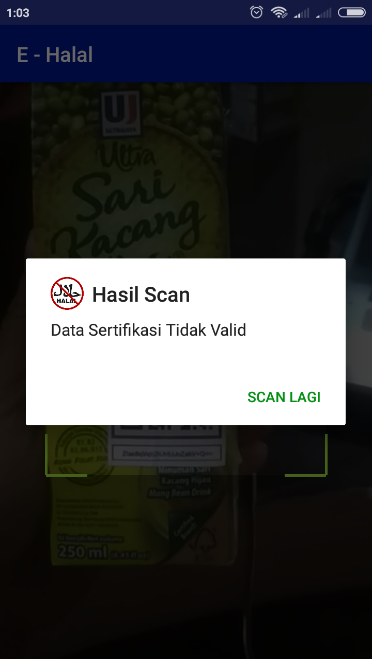
Gambar 3.7 Poses Scanning Qr Code

Gambar diatas adalah proses scanning Qr code dengan aplikasi dimana Qr code mengandung data no sertifikat yang terenskripsi, setelah proses scanning merekam data dan akan di kirim keserver untuk proses deskripsi, dan jika data benar maka sistem melalui aplikasi akan menampilkan hasil sesuai data sertifikat, sebagai berikut :

* Hasil scan

Gambar 3.8 Hasil Scan

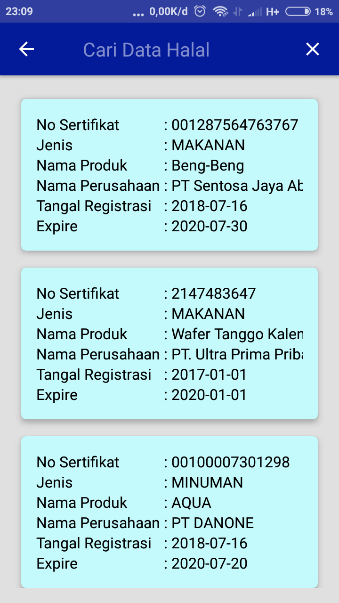
Gambar 3.8 adalah hasil dari scanning Qr code jika data nya valid dan akan menampilkan data detail sertifikasi yang diambil dari database server.

* Hasil Scan jika Data tidak Valid

Gambar 3.9 Hasil Scan Tidak valid

Gambar diatas menunjukan hasil scan jika kode yang di scan adalah kode tidak teregistrasi di database.

* Menu Input Kode



Gambar 3.10 Tampilan Pencarian Data(input kode)

Gambar 3.10 diatas adalah tampilan menu input kode dimana kita bisa melakukan pencarian data berdasarkan kode yang tercantum di Qr code tersebut, yang nanti akan ditempel pada kemasan produk

1. KESIMPULAN DAN SARAN
2. Kesimpulan

Berdasarkan uraian dan pembahasan diatas penulis dapat menyimpulkan beberapa kesimpulan diantaranya adalah sebagai berikut :

1. Dengan adanya aplikasi berbasis mobile konsumen dapat mengetahui kehalalan dan masa berlaku sertifikat halal secara praktis aman dan terpercaya.
2. Algoritma AES pada aplikasi ini berfungsi sebagai salah satu solusi keamanan data halal yang mengenskripsi no sertifikat pada database. Sehingga data tidak mudah di manipulasi.
3. Dengan menggunakan Algoritma *Advance Encryption Standard* 128 yang di implementasikan pada system dan di simpan dalam bentuk QR code terenskripsi sehingga keaslian data sertifikasi dan validasi akan aman.

1. Saran

Dan tentunya aplikasi yang penulis kembangkan masih mempunyai beberapa kekurangan dan ada beberapa saran untuk pengembangan kedepanya diantaranya adalah sebagai berikut :

* + 1. Untuk pengembangan selanjutnya diharapkan data yang ada dapat ditambahkan sesuai dengan data yang ada pada lembaga terkait.
    2. Diharapkan aplikasi ini dapat diterapkan di Badan Pengelola Jaminan Produk halal dikarnakan konsep keamanan data yang telah di enskripsi sehingga data aman dan tidak mudah di manipulasi
    3. Meningkatkan tingkat keamanan dengan menamah panjang kunci AES dari 128 menjadi 256 atau lebih tinggi sehingga kemanan akan lebih baik.

Penambahan fitur yang mampu menerima krtitikan, masukan atapupn aduan dari konsumen

DAFTAR PUSTAKA

[1] Adhi, J. S., (2005), Kriptografi dengan Algoritma Rijndael untuk Penyandian Data, Skripsi, Yogyakarta: Universitas Kristen Duta Wacana.

[2] Aji, Diana, Nasrul. 2016. Perbadingan Algoritma DES dan Algoritma AES pada Teknologi QR Code. UNIVERSITAS BINA DARMA

[3] Ajini, Arun, 2015, *Qr Code Based Data Transmision in Mobile Devices Using AES Encryption*. Department Of Rlectronic And Communication Sree Budha College Of Enggineering.

[4] Boediono. (1998). Dampak Krisis Ekonomi Terhadap Pendidikan. Jakarta:

Pusat Penelitian Sains dan Teknologi UI.

[5] Dony, A. (2005), Kriptografi Keamanan Data dan Komunikasi, Yogyakarta: Penerbit Andi Offset.

[6] Egi, Ryandi. 2015 Penerapan Metode Smart Authentication Dalam Layanan E-Banking Menggunakan Two Channel Authentication Dan QR Code Pada Perangkat Mobile Android. SEKOLAH TINGGI SANDI NEGARA

[7] Kumar Kolli, naveeen 2017, Implementatition Of Secure Payment Transaction Using AES Encryption With Extended Visual Cryptograhpy. Department Of Computing Sciences Texaa A&M University – Corpus Christi Corpus Christi, Texas

[8] Khaidir.2004.Microsoft Visual Basic 6.0. Jakarta : Elex Media Komputindo

[9] Knight, John F. 2001. Family Medical Care Volume 4. Bandung: Indonesia Publishing House.

[10] Munir, Renaldi. (2005). Algoritma dan Pemrograman dalam Bahasa Pascal dan C edisi 3, Bandung : Informatika Bandung.

[11] Nugroho, Adi . 2005. Rational Rose Untuk Pemodelan Berorientasi Objek, Penerbit : Informatika, Bandung.

[12]Supriyanto.2005.Perancangan Aplikasi.Surabaya : Widyastana

[13] Tim Kemenag,, 2003 Daftar Produk halal Indonesia, Kementrian Agama, bagian sarana dan prasarana produk halal.

[14] Voni, gani, Antonius, 2017, Enskripsi dan deskripsi Algoritma Advance Encryption Standard 256 Untuk Semua Jenis File. Universitas Kristen Duta Wacana.