PENGGUNAAN QR CODE BERBASIS KRIPTOGRAFI ALGORITMA AES ADVANCED ENCRYPTION STANDARD UNTUK ADMINISTRASI REKAM MEDIS

Ferdiansyah[1], Asep Id Hadiana[2,] Fajri Rakhmat Umbara [3]

[1,2]*Teknik Informatika, Universitas Jenderal Achmad Yani*

Jalan Terusan Jend. Sudirman, Cibeber, Kec. Cimahi Sel., Kota Cimahi, Jawa Barat 40531

[1]ferdiansyah@student.unjani.ac.id

[2]asep.hadiana@lecturer.unjani.ac.id

[3]fajri.umbara@gmail.com

Abstrak— **Data Administrasi dalam kesehatan dapat mengandung beberapa informasi penting, seperti identitas pasien, dokter, bahkan fasilitas kesehatan. Kemanan data diperlukan untuk menjaga kerahasiaan dan mencegah pihak yang tidak berwenang menyalahgunakan data tersebut. Tujuan dari penelitian ini adalah untuk menjawab gap yang ada dengan Penggunaan QR Code mengamankan Kemudian QR Code tersebut dibagian Dokumen untuk Manajemen Administrasi. Pada penelitian ini, pesan data Informasi rahasia disematkan ke QR code berbasis Kriptografi dengan menggunakan Metode AES Advanced Encyrption Standard. QR code akan memperbaiki kesalahan yang dihasilkan prosedur penyematan rahasia ke dalam dokumen, kemudian QR code dapat memvalidasi untuk menampilkan data. Penulis melakukan pengujian dengan menggunakan metode brute force dan Pengujian AES untuk memastikan keamanan Aplikasi ini berjalan sebagaimana mestinya dalam mengamankan data tersebut. Hasil dari penelitian ini adalah QR code dapat mengamankan dokumen data Administrasi Rekam Medis dengan menggunakan metode AES. Dengan ini diharapkan dapat mengurangi potensi kebocoran data Administrasi Rekam Medis secara signifikan. Kesimpulan dari Penulis telah menyajikan pendekatan untuk mengamankan data menggunakan teknologi menyimpan yang digunakan untuk otentikasi saat melakukan request data administrasi. Penggunaan metode keamanan AES Advanced Encyrption Standard ini memberikan keuntungan dalam penggunaan yang mudah dan penggunaan sumber daya yang efisien**

Kata kunci— ***kriptografi, Advanced Encryption Standard, QR Code, validasi.***

Abstract—**Administrative data in health can contain some important information, such as the identity of patients, doctors, and even health facilities. Data security is needed to maintain confidentiality and prevent parties who do not misuse the data. The purpose of this study is to answer the gap that exists with the use of QR Code Documents. Then the QR Code is divided for Administrative Management. In previous studies using QR codes based on Cryptography for administrative data systems in the health sector. In this study, confidential information data messages are embedded into a Cryptographic-based QR code using the AES Advanced Encryption Standard Method. The QR code will correct the error generated by the secret embedding procedure into the document, then the QR code can validate to display the data. The author conducted testing with brute force and AES methods to ensure the security of the application running properly in the data. The result of this research is that the QR code can enter Medical Record Administration data documents using the AES method. With this, it is expected to significantly reduce the potential for data leakage from the Medical Record Administration. The conclusion of the authors in this study aims to perform data administration by using a QR Code based on Cryptography. The author has presented an approach to accessing data using the storage technology used for authentication when performing data administration requests. The use of this AES Advanced Encryption Standard security method provides the advantages of ease of use and efficient use of resources**

.

Keywords— ***cryptography, Advanced Encryption Standard, QR code, validation.***

I. PENDAHULUAN

QR Code mampu menyimpan semua jenis data, seperti data angka/numerik, alpanumerik, biner [1]. Selain itu QR Code memiliki tampilan yang lebih kecil daripada barcode. Oleh karena itu, jika simbol QR Code kotor ataupun rusak, data dapat disimpan dan dibaca, Tiga tanda berbentuk persegi di tiga sudut memiliki fungsi agar simbol dapat dibaca dengan hasil yang sama dari sudut manapun. Untuk mengantisipasi terjadinya pemalsuan dokumen, maka dilakukan pengamanan dengan cara menyisipsikan suatu objek pengenal seperti ID, atau tanda tangan yang digunakan untuk mencocokkan konten yang tertulis pada dokumen,[2] yang kemudian akan disisipkan dan diproses sedemikian rupa menjadi sebuah kode yang akan diidentifikasi dan dicocokkan[3]. QR Code merupakan teknik yang mengubah data tertulis menjadi kode 2 dimensi yang tercetak kedalam suatu media yang lebih ringkas. Dengan QR Code, informasi keaslian dokumen tersebut dibuat menjadi lebih sederhana dan simpel tanpa mengetikkan informasi kode atau surat keterangan pada dokumen tersebut.

Pada bidang Kesehatan[4], Potensi teknologi informasi telah berperan penting dan senantiasa mengalami modernisasi. Hal ini dapat dilihat dari adanya akses luas dalam hal memperoleh informasi yang dibutuhkan dengan mudah[5]. Dengan adanya Sistem dalam bidang khususnya Kesehatan, Perubahan fungsi mulai bergeser pada sebuah kebutuhan dan Kerahasiaan terhadap data Administrasi[6][7].

Oleh sebab itu dibutuhkan sebuah cara yang dapat menjaga kerahasiaan dan keamanan pada perlindungan informasi dari pihak yang tidak sah. Salah satu mekanisme untuk meningkatkan keamanan data[8] adalah dengan menggunakan teknik kriptografi. kriptografi [9]salah satunya adalah Algoritma Advance Encryption Standard[10], data yang disimpan ke dalam QR code kemudian disisipkan ke

dokumen sehingga tidak mudah dibaca.[11] Proses Enkripsi adalah proses yang dilakukan untuk merubah suatu informasi sehingga tidak dapat dibaca. Sebaliknya, Proses dekripsi merupakan suatu proses yang mengembalikan informasi yang sudah dienkripsi menjadi bisa dibaca Kembali.[12]

Telah banyak penelitian-penelitian yang membahas Metode algoritma AES Advanced Encryption Standard Contohnya seperti data Administrasi yang berisi data yang berkaitan dengan kesehatan milik banyak pasien.[13] Terdapat beberapa kasus kebocoran data yang pernah terjadi di dunia. Salah satunya adalah yang terjadi pada perusahaan penyedia pencarian Sistem bernama JustDial yang menyebabkan 100 juta data Administrasi bocor. Data pengguna yang bocor antara lain nama, email, nomor ponsel, alamat, jenis kelamin, tanggal lahir, foto, pekerjaan, dan nama perusahaan yang bekerja dengan perusahaan tersebut. Kejadian ini disebabkan oleh Sistem Informasi yang masih menggunakan Aplikasi [14] RFID Radio Frequency Identity yang tidak terproteksi dan hanya sedikit digunakan oleh perusahaan namun dibiarkan tetap aktif dipakai dalam bidang Industri dan Kependudukan, Kebocoran data ini ditemukan oleh seorang peneliti keamanan bernama Kentaro Fukuchi yang sedang melakukan pengembangan terhadap QR code,[15] Lalu kemudian Kentaro Fukuchi melakukan pembaruan tentang QR code. Pada penelitian ini Penulis akan menggunakan Metode Algoritma AES Advanced Encryption Standard ini sebagai bukti tingkat keamanan yang baik, bisa dibuktikan dengan penelitian DES Data Encryption Standard pada penelitian sebelumnya membahas tentang legalisasi ijazah[16] dengan kriptografi visual untuk enkripsi dan dekripsi pada RFID Code dengan metode DES Data Encryption Standard tersebut.

Namun dari penelitian-penelitian tersebut masih jarang dan hampir sudah tidak ada tentang penelitian Data Encyrption Standard ini yang menerapkan keamanan yang baik terhadap Penggunaan metode tersebut.[12] Kemudian Penulis melakukan Pembaruan [17]pada implementasi QR code data Administrasi Rekam Medis ini dengan kekurangan memiliki celah keamanan yang disebabkan oleh tidak adanya sistem otentikasi bawaan yang dapat mengancam privasi data yang ditransmisikan[8]. Masalah ini penting untuk diatasi untuk memastikan data yang ditransformasi terhindar dari penyalahgunaan oleh pihak yang tidak bertanggung jawab. Untuk mengatasi masalah tersebut metode Penulis mengusulkan metode AES Advance Encryption Standard digunakan untuk mengamankan [18] Teknik Enkripsi dan Dekripsi antara Fasilitas Kesehatan Klinik dengan Bagian Apoteker[19]. Tujuan dari penelitian ini adalah untuk menjawab gap yang ada dengan Penggunaan QR Code mengamankan Kemudian QR Code tersebut akan ditempel dibagian Dokumen untuk Manajemen Administrasi.[20] Hasil dari penelitian ini akan bermanfaat dalam pengamanan data Administrasi, khususnya data yang bersifat rahasia seperti data Administrasi Rekam Medis.

A. Rumusan Masalah

Terdapat celah keamanan ketika data Administrasi mengirimkan data melalui Sistem yang mengamankan data dengan Sistem Aplikasi tanpa pengamanan data seperti otentikasi yang menyebabkan keamanan data Administrasi dapat ditembus dengan mudah sehingga diperlukan pengamanan QR code dan login dengan harapan dapat menghasilkan keamanan yang lebih modern dan aman.

B. Tujuan

Tujuan yang ingin dicapai pada penelitian ini adalah untuk menyelesaikan masalah keamanan data Administrasi Reakm Medis dengan membuat QR Code yang berfungsi untuk mengelola hak akses dan untuk melihat seluruh data Administrasi rekam medis dengan cara menerapkan dan kemudian memindai QR code didalam dokumen menggunakan perangkat kamera yang tersedia dengans metode keamanan AES *Advanced Encryption Standard*.

C. Ruang Lingkup

Aplikasi QR Code dibangun untuk mengelola hak akses membuka data Administrasi Rekam Medis dari Fasilitas Kesehatan dengan menerapkan QR code metode keamanan AES Advanced Encryption Standard..

II. LANDASAN TEORI

Kombinasi keamanan sistem Aplikasi merupakan hal yang menarik dan banyak diteliti oleh peneliti-peneliti di bidang keamanan data. Tercatat dari tahun 2016-2021 terdapat sekitar 38.994 publikasi yang teridentifikasi di Science Direct mengenai keamanan ini. Hal ini berdampak pada meningkatnya jumlah penelitian tersebut pada berbagai bidang, seperti bidang kesehatan.

Tinjauan pustaka pada penulis ini menguraikan tentang teori prinsip dasar penelitian terdahulu tentang bagaimana tujuan utama dari Metode AES Advanced Encryption Standard sebagai salah satu metode dalam mengamankan suatu sistem.

A. AES (Advanced Encryption Standard)

AES (Advanced Encryption Standar) adalah lanjutan dari algorima enkripsi standar DES (Data Encryption Standar) yang masa berlakunya dianggap telah usai karena faktor keamanan Algoritma ini termasuk jenis simetri yang disebut juga sebagai algoritma konvensional, yaitu algoritma yang menggunakan kunci enkripsi dan kunci dekripsi yang sama[7] AES menggunakan sandi blok kunci simetris dengan ukuran kunci bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Pemerintah Amerika Serikat telah mengadopsi AES sebagai standar enkripsi. Standar ini terdiri dari 3 blok cipher, yaitu AES-128, AES-192, dan AES-256 yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. [8]AES telah dianalisis secara luas dan sekarang digunakan di seluruh dunia, seperti halnya dengan pendahulunya[9], *Data Encryption Standard* (DES)[10]

B. Konsep QR Code

QR QR Code adalah kode batang dua dimensi yang merupakan pengembangan barcode barcode sebelumnya. Jika data barcode lama disimpan secara horizontal, tetapi QR Code data disimpan secara horizontal dan vertikal. Dengan kemampuan untuk menyimpan dalam dua dimensi QR Code tentunya bisa menyimpan lebih banyak data dan variatif daripada barcode. Itu jenis data yang dapat disimpan di QR Code adalah termasuk mode Numerik, mode Alfanumerik, 8-bit mode byte, dan Mode Kanji.

Algoritma enkripsi yang digunakan adalah AES128 dengan ECB sebagai mode buku kode elektronik. Itu

Parameter Kode QR menggunakan Kode QR PHP perpustakaan, seperti format keluaran dalam PNG[12], Tingkat ECC adalah Tengah, ukuran gambar adalah 6, dan ukuran bingkai adalah 2. target format file objek harus dalam format JPG / JPEG, PNG, dan GIF. Format file keluaran dalam JPG / JPEG. lebar maksimum file keluaran adalah 2126 dan 1414 untuk tinggi maksimal

Tabel 1 Karakterisitik Simbol QR code

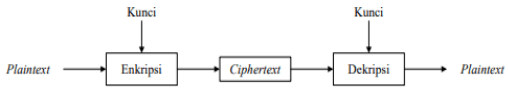
Numerik Data 7890 Karakter
Alphanumeric data 4296 Karakter
8-bit byte data 2953 Karakter
Karakter Kanji 1817 Karakter

C. Penggunaan QR Code

Bagian QR code yang terdiri dari pattern, separator, timming pattern, alignment pattern[4]Dan Disimpan pada 3 khusus di bagian kanan atas, kiri atas dan kiri bawah. Pola finder memiliki perbandingan (1.1.3.1.1) Separator yaitu Ditempatkan diantara pola dengan posisi format terang. Timing Patterns Berada pada ujung pola deteksi yang memotong dari satu ujung deteksi dengan ujung lainnya. Berbentuk garis pembatas berisi nilai 1 dan 0. Alignment Patterns Pola penyelaras posisi dengan finder pattern. [8] Encoding Region Wilayah dari data yang dimasukkan dan di encoding dalam bentuk QR code Format Information: Menginformasikan kerusakan QR Code pada level tertentu, Version Information Versi dari QR Code. Versi terkecil memiliki 21x21 modul dan terbesar 177x177 modul 9 Quiet Zone: Zona tidak ada pola atau tanda, berada pada 4 sisi gambar QR Code. Jika sebuah QR Code tidak terdapat zona ini, maka ada kemungkinan QR code sulit terbaca

D. Kriptografi

Aplikasi kriptografi juga banyak digunakan di improvisasi pembuatan QR Code seperti yang menggunakan *Advance Encryption Standard (AES)* enkripsi pada sistem legalitas digital dan menggunakan modifikasi Algoritma SHA dalam pembuatan QR Code. Mencetak perlindungan dokumen dapat menggunakan kombinasi QR Code dan tanda tangan digital tak terlihat, Sedangkan pada teknik lainnya dengan menggabungkan teknik watermark dan QR Code [21][22] dengan memasukkan gambar ke dalam gambar QR Code, dapat dilihat alur atau Proses pada Gambar 1



Gambar 1 Kriptografi

Kriptografi Bertujuan untuk memberikan layanan pada aspek keamanan yaitu:

1) Kerahasiaan (Confidentiality) yaitu menjaga pesan tidak dapat di baca oleh pembaca oleh pihak yang tidak berhak melihat

2) Integritas Data (data Integrity) yaitu memberikan jaminan bahwa untuk tiap pesan tidak akan mengalami perubahan dari saat di buat atau di kirim, sampai data tersebut dibuka oleh penerima data

3) Otentikasi (Authentication) yaitu berhubungan dengan identifikasi yang berkomunikasi kebenaran sumber data

4) Nirpenyangkalan (Non Repudaiation) yaitu memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seorang tertentu sehingga apabila ada orang yang mencoba mengakui memiliki dokumen tersebut, dapat dibuktikan kebenarannya dari pengakuan orang tersebut .

E. Autentikasi

Dalam hal ini autentikasi merupakan sebuah proses identifikasi yang dilakukan oleh pihak yang satu terhadap pihak yang lain ataupun sebaliknya dengan melakukan berbagai proses identifikasi untuk memastikan keaslian dari informasi yang diterima.

F. Password (Kata Sandi)

Penulis telah melakukan eksperimen untuk mencoba menentukan kebiasaan pengguna yang khas dalam memilih kata sandi ketika tidak ada batasan yang diberikan pada pilihan mereka. Hasil mengecewakan, kecuali untuk orang jahat. Dalam koleksi dari 2.339 kata sandi yang dikumpulkan dari banyak pengguna selama jangka waktu yang lama. Tabel Spesifikasi dapat dilihat pada Tabel 2.

Tabel 2 Password Akses Spesifikasi

15 adalah karakter ASCII tunggal;
72 adalah string dari dua karakter ASCII;
464 adalah string dari tiga karakter ASCII;
477 adalah string dari empat alfamerik;
706 adalah lima huruf, semua huruf besar atau semua huruf kecil;
605 terdiri dari enam huruf, semuanya huruf kecil

III. PERANCANGAN

Dalam Bab III ini perancangan menjelaskan pada Perancangan perangkat lunak yaitu Perancangan Library QR code, Perancangan Otentikasi, Perancangan Kamera QR code perangkat lunak, Class Diagram dan Usecase Diagram dan Aplikasinya, hingga Rancangan Antarmuka pengguna dari perangkat lunak yang dibangun.

A. Perolehan Data

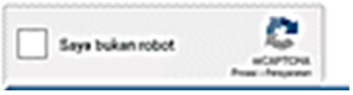
Pengumpulan Data yang diperoleh dari Fasilitas Kesehatan (Faskes) akan dikumpulan dan selanjutnya diolah penulis. Pengumpulan data ini dilakukan selama kurang lebih 2-4 bulan. data ini dilakukan observasi langsung terhadap data yang diperoleh seperti Pemilik, dan bagian Staff Fasilitas Kesehatan, Untuk data sekunder, Data sekunder berupa data obat lainnya yang diperoleh dari Fasilitas Kesehatan tersebut, Persediaan data saat ini dilakukan untuk mengetahui jumlah Obat dan data rekam medis untuk menguraikan daftar rekam medis Fasilitas Kesehatan

Sistem otentikasi berfungsi untuk memvalidasi request yang berasal dari admin atau user guna memastikan terdaftar

pada database dan memiliki hak akses untuk mengakses data rekam medis. Untuk membuatnya diperlukan perancangan algoritma dan sequence diagram.

B. Spesifikasi Kebutuhan Aplikasi QR code

Spesifikasi ini menjelaskan tentang Perancangan Library QR Code, penulis menerapkan beberapa library untuk diterapkan dan digunakan dalam bidang Sektor Kesehatan yaitu Administrasi Rekam Medis. Library ini berfungsi untuk penerapan dan bagian dari perancangan QR code yang dibuat untuk menyisipkan QR code tersebut untuk dokumen Administrasi Rekam Medis, Kemudian pada Library Captcha Spesifikasi ini suatu bentuk uji tantangan yang digunakan dalam keamanan untuk memastikan bahwa serangan tidak dapat dihasilkan oleh suatu komputer dan jaringan, dilihat dari Gambar 2 dan Library QR code Tabel 3



Gambar 2 Layanan Captcha

Tabel 3 Library QR Code

Library QR Code
include $QR_BASEDIR."qrconst.php";
include $QR_BASEDIR."qrconfig.php";
include $QR_BASEDIR."qrtools.php";
include $QR_BASEDIR."qrspec.php";
include $QR_BASEDIR."qrimage.php";
include $QR_BASEDIR."qrinput.php";
include $QR_BASEDIR."qrbitstream.php";
include $QR_BASEDIR."qrsplit.php";
include $QR_BASEDIR."qrrscode.php";
include $QR_BASEDIR."qrmask.php";
include $QR_BASEDIR."qrencode.php";

C. Perancangan Spesifikasi Kamera QR code

Pada Penggunaan QR code ini dibutuhkan Komunikasi data pada QR code yang disematkan dalam dokumen Aplikasi dengan webcam/kamera perangkat lunak untuk melakukan Pemindaian QR code, salah satunya Framework diantaranya adalah webcam pemindai, Library QR code untuk memindai dan menyisipkan QR code untuk dokumen, menurut penulis secara definisi plugin adalah Pemrograman komputer atau kerangka kerja perangkat lunak dimana perangkat lunak ya fungsional generik, dapat diubah secara selektif oleh kode yang ditulis pengguna tambahan, sehingga menyediakan perangkat lunak. Kemudian Penulis menggunakan Plugin Kamera khusus tersebut yang berfungsi untuk memindai QR code aplikasi. Kemudian pada bagian Captcha ini terdapat bagian Secret Key dan Site Key, artinya pada captcha ini terdapat kunci rahasia untuk verifikasi dan validasi, jika box bagian tidak di klik maka teridentifikasi Robot, jika melakukan aksi klik dilakukan oleh user maka teridentifikasi bahwa bukan robot. Untuk Secret Key dan Site Key berfungsi untuk identifikasi pemanggilan verifikasi fungsi API dari Developers.google.com, dapat dilihat pada

Tabel 4 Site dan Secret key Captcha

```
$secret_key =
"6LcRo7QbAAAAAGUxiqlFSqIyGjR0hMBlRuRH3ugi";
<div class="form-group">
            <div class="g-recaptcha"
$data-
sitekey="6LcRo7QbAAAAAI6ePvxTerTjOZ2cgpQm3
V-ynExK">
             </div>
<script
src='https://www.google.com/recaptcha/api.js'></
script>
```

IV. IMPLEMENTASI DAN PENGUJIAN

Pada implementasi terbagi menjadi empat bagian, yaitu implementasi sistem otentikasi username dan kata sandi, Generator QR Code, Implementasi Spesifikasi Kebutuhan Aplikasi QR Code dan Implementasi perangkat lunak.

A. Implementasi Basis Data

Basis data digunakan untuk menyimpan data yang berkaitan dengan sistem otentikasi token akses. Database Management System (DBMS) yang digunakan adalah MariaDB dengan versi 10.4.18. Pada basis data ini terdapat 3 tabel yaitu tabel Admin dan tabel Dokter, Tabel Obat.

1) Tabel Admin

Tabel Admin memiliki beberapa field utama yaitu idadmin username, password, namalengkap Tabel Admin dapat dilihat pada Gambar 3

#	Nama	Jenis	Penyortiran	Atribut	Tak Ternilai	Bawaan	Komentar	Ekstra	Tindakan
1	idadmin	int(5)			Tidak	Tidak ada		AUTO_INCREMENT	Ubah Hapus
2	username	text	utf8_general_ci		Tidak	Tidak ada			Ubah Hapus
3	password	text	utf8_general_ci		Tidak	Tidak ada			Ubah Hapus
4	namalengkap	text	utf8_general_ci		Tidak	Tidak ada			Ubah Hapus

Gambar 3 Tabel Admin

2) Tabel Data Medis

Tabel Data Medis memiliki beberapa field yaitu id, no_reg, dokter, jns_kelamin, jns_layanan, pasien, jns_obat, kd_obat, tgl_periksa, diagnosa, status_byr, dan biaya. Terdapat juga field tambahan yaitu tgl_periksa yaitu dengan jenis tipe date menyimpan tanggal, bulan, dan tahun pembuatan data. Tabel Data Medis dilihat dari Gambar 4

#	Nama	Jenis	Penyortiran	Atribut	Tak Ternilai	Bawaan	Komentar	Ekstra	Tindakan
1	id	int(10)			Tidak	Tidak ada		AUTO_INCREMENT	Ubah Hapus Lainnya
2	no_reg	varchar(10)	utf8_general_ci		Ya	NULL			Ubah Hapus Lainnya
3	dokter	varchar(40)	utf8_general_ci		Ya	NULL			Ubah Hapus Lainnya
4	jns_kelamin	varchar(40)	utf8_general_ci		Ya	NULL			Ubah Hapus Lainnya
5	jns_layanan	varchar(40)	utf8_general_ci		Ya	NULL			Ubah Hapus Lainnya
6	pasien	varchar(40)	utf8_general_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
7	jns_obat	varchar(40)	utf8_general_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
8	kd_obat	varchar(40)	utf8_general_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
9	tgl_periksa	date			Tidak	Tidak ada			Ubah Hapus Lainnya
10	diagnosa	varchar(40)	utf8_general_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
11	status_byr	varchar(40)	utf8_general_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
12	biaya	int(10)			Tidak	Tidak ada			Ubah Hapus Lainnya

Gambar 4 Tabel Data Medis

3) Tabel Data Obat

Tabel Obat memiliki beberapa field yaitu kd_obat, nm_obat, jns_obat, quantity, dapat dilihat pada Gambar 5

Struktur tabel | Tampilan hubungan

#	Nama	Jenis	Penyortiran	Atribut	Tak Ternilai	Bawaan	Komentar	Ekstra	Tindakan
1	kd_obat	int(12)			Tidak	Tidak ada			Ubah Hapus Lainnya
2	nm_obat	varchar(50)	latin1_swedish_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
3	jns_obat	varchar(20)	latin1_swedish_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
4	quantity	int(100)			Tidak	Tidak ada			Ubah Hapus Lainnya

Gambar 5 Tabel Data Obat

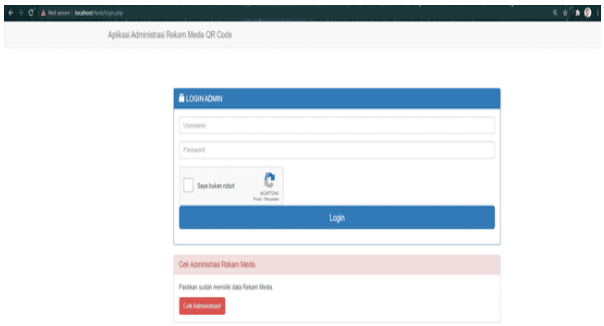
B. Implementasi Keamanan Aplikasi QR code

Implementasi Aplikasi QR code ini dilakukan berdasarkan perancangan yang telah dilakukan pada Bab III dan di deploy. Aplikasi QR code ini mengimplementasikan QR code dan mengirimkan datanya dalam format dokumen. dengan bahasa pemorgraman PHP versi 8.0 dipilih untuk pengembangan Aplikasi QR code, versi ini banyak digunakan oleh pengembang perangkat lunak. Bahasa pemrograman dan framework serta plugin ini untuk membantu memudahkan dalam pembuatan QR code .

Aplikasi QR code ini memiliki sebuah layanan yang dapat digunakan oleh Admin untuk mengambil seluruh data Administrasi rekam medis maupun satu data spesifik berdasarkan id. Pada penelitian ini diimplementasikan pada perangkat lunak, untuk memberikan gambaran nyata mengenai penerapan penelitian ini

1) Login Captcha

Layanan Captcha Login merupakan layanan yang berfungsi untuk mengambil data login Hak Akses untuk mengamankan login dari serangan brute force, secara keseluruhan dari file rekam medis yang tersimpan di-direktori root. Layanan lihat rekam medis dilihat dari Gambar 6



Gambar 6 Halaman Antarmuka Generator QR Code

2) Implementasi Kamera Webcodecam

Layanan webcodecam QR code ini merupakan layanan yang berfungsi untuk plugin mengambil data QR code satu baris data secara spesifik berdasarkan id dari file QR code yang sudah kemudian melakukan pemindaian untuk membuka Data yang ada didalam QR code tersebut, Lalu data medis yang dibuat dengan dokumen yang diamnakan akan tersimpan di direktori Program File. Layanan Webcodecam QR code dilihat dari Gambar 7

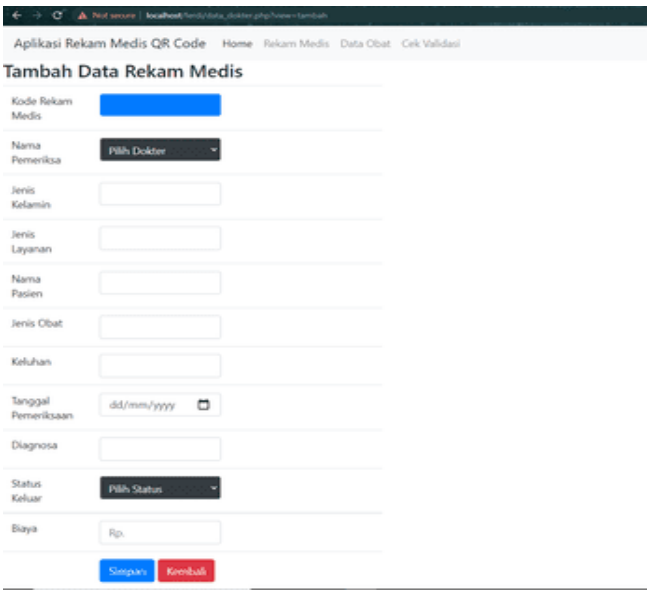
Gambar 7 Implementasi WebcodeCam

C. Implementasi Perangkat Lunak

Perangkat lunak sampel adalah yang menerapkan semua layanan yang tersedia pada Sistem Administrasi Rekam Medis. Perangkat lunak sampel melakukan input dan menampilkannya. Perangkat lunak ini dibangun menggunakan bahasa pemrograman Php dan JavaScript. Terdapat beberapa library yang digunakan yaitu library phpqrcode , library qr code, library captcha dan untuk tampilan antarmuka yaitu Bootstrap 4. Terdapat dua halaman yaitu daftar rekam medis yang secara keseluruhan, dan Hasil detail rekam medis yang menampilkan baris data rekam medis yang dipilih berdasarkan id yang sudah diinput dari menu Rekam Medis.

1) Halaman Antarmuka Tambah Data

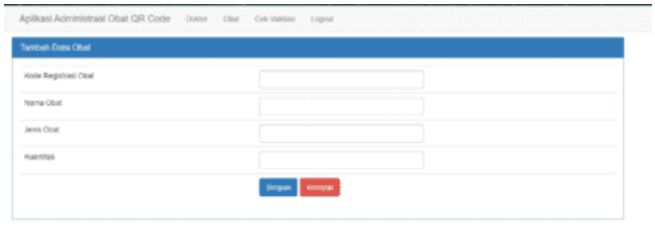
Halaman ini memiliki fitur menampilkan data rekam medis secara keseluruhan melalui tabel. Data yang ditampilkan adalah Nomor Rekam Medis, Nama Pemeriksa, Jenis Kelamin, Jenis Pelayanan, Nama Pasien, Obat Utama, Keluhan, Tanggal Pemeriksaan , Diagnosa, Status Keluar, Biaya. Tabel yang digunakan merupakan tabel yang berasal dari library BS4. Dengan tabel ini, pengguna dapat melakukan pengurutan, baris data maksimal yang ditampilkan pada setiap halaman tabel. Antarmuka halaman daftar Tambah data rekam medis dilihat dari Gambar 8



Gambar 8 Halaman Antarmuka Rekam Medis

2) Halaman Antarmuka Data Obat

Halaman detail Antarmuka Obat memiliki fitur untuk menampilkan dan Menambahkan data obat secara spesifik berdasarkan dari data yang diketik Data yang ditampilkan adalah kode obat, Nama obat, Jenis obat, dan Kuantitas. Antarmuka halaman Obat dapat dilihat pada Gambar 9



Gambar 9 Halaman Antarmuka Data Obat

3) Halaman Antarmuka Cetak Dokumen

Halaman Cetak Dokumen rekam medis memiliki fitur halaman tampilan secara spesifik diantaranya adalah QR code tersedia dibagian pojok bawah kiri dari data yang pilih, Data yang ditampilkan adalah Surat Keterangan Sakit. Antarmuka Cetak Dokumen rekam medis dilihat dari Gambar 10

Gambar 100 Halaman Antarmuka Cetak Dokumen

D. Pengujian Perangkat Lunak

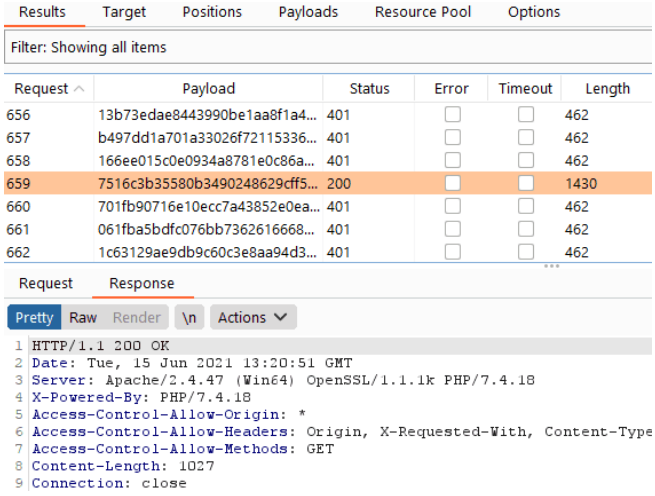
Pengujian dilakukan pada aplikasi yang dibangun agar bekerja dengan baik dan sesuai dengan kebutuhan yang didefinisikan dan untuk mencari kesalahan terjadi pada aplikasi yang dioperasikan. Pengujian dilakukan terbatas pada pengujian keamanan Sistem Aplikasi QR code pada bagian login dan metode AES Advance Encryption Standard. Pengujian yang dilakukan yaitu brute force.

Target uji pada penelitian ini yaitu Aplikasi QR Code Berbasis Kriptografi yang menerapkan metode keamanan Advanced Encyrption Standard. Pengujian Aplikasi ini akan menggunakan spesifikasi perangkat keras dan burp suite sebagai tools software tambahan untuk pengujian brute force.

E. Pelaksanaan Pengujian

Pengujian dengan metode brute force juga dilakukan karena metode ini menggambarkan kasus di dunia nyata di mana pihak yang tidak bertanggung jawab mencoba secara acak berulang kali hingga hingga menemukan Kata Sandi yang valid yang dapat digunakan untuk mengakses data pada Aplikasi QR Code.

Untuk melakukan pengujian ini, penulis menggunakan perangkat lunak alat bernama Burp Suite, yang dapat memindai dan mengumpulkan data serangan aplikasi QR code. Tahap pertama adalah menentukan target yaitu Aplikasi QR code. Kemudian penulis memutuskan untuk menggunakan 1.000 kata sandi teratas yang paling banyak digunakan dari daftar Most Common Passwords dari situs www.passwordrandom.com. Kumpulan kata sandi ini akan digunakan untuk melakukan serangan brute force melalui parameter.



Gambar 11 Hasil Pengujian Brute Force

Pengujian ini diselesaikan dalam 4 menit 10 detik dan menghasilkan hasil yang valid pada iterasi ke 659, seperti yang dilihat dari Gambar 11 Setiap pengujian dapat menghasilkan angka yang berbeda tergantung pada kompleksitas dan waktu akses. Metode pengujian ini dapat menjadi lebih sulit untuk dilakukan ketika penguji/penyerang tidak mengetahui jumlah karakter kata sandi yang digunakan karena harus melakukan serangan ini beberapa kali untuk mendapatkan jumlah karakter yang tepat.

Pada pengujian bagian pada keamanan AES dimana pengujian ini menghasilkan cipher dengan kunci ekspansi yang di enkrip password yang digunakan penulis, pada pengujian ini dilakukan dengan password default (admin),

kemudian password tersebut transformasi berubah cipher, Lalu Cipher dan Key tersebut bisa dilakukan proses dekrip, artinya pada hasil pengujian ini bisa dilakukan telah dibuktikan bahwa metode AES Advance Encryption Standard ini layak untuk dipakai beberapa tahun ke depan, seperti yang dilihat pada gambar 12

Gambar 122 Implementasi Pengujian AES

F. Evaluasi Hasil Pengujian

Berdasarkan hasil dari pelaksanaan pengujian dengan menggunakan metode brute force testing yang telah dilakukan pada setiap fungsi kelemahan perangkat lunak, dapat disimpulkan bahwa secara keseluruhan perangkat lunak berjalan dengan baik dan sesuai antara hasil yang diharapkan dengan respon sistem. Hal tersebut menunjukkan bahwa perangkan lunak telah memenuhi kebutuhan fungsional yang telah ditetapkan pada tahap sebelumnya.

V. KESIMPULAN

Penelitian ini bertujuan untuk mengamankan data dengan menggunakan QR Code berbasis Kriptografi. Penulis telah menyajikan pendekatan untuk mengamankan data menggunakan teknologi menyimpan yang digunakan untuk otentikasi saat melakukan request data. Penggunaan metode keamanan AES Advanced Encyrption Standard ini memberikan keuntungan dalam penggunaan yang mudah dan penggunaan sumber daya yang efisien. Temuan ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa QR Code berbasis Android dan Sistem QR code yang terintegrasi sektor pendidikan untuk keamanan data, Meskipun dalam penelitian ini pengamanan yang dilakukan hanya terhadap Administrasi data rekam medis menggunakan QR code, namun kasus lain juga dapat menggunakan pendekatan ini.

Penulis telah melakukan pengujian keamanan yang dibangun dengan melakukan serangan brute force. Dari pengujian ini, penulis menemukan bahwa Sistem Aplikasi yang dibangun dapat menangkal serangan dari brute force namun belum dapat sepenuhnya menangkal serangan tersebut jika penyerang mengetahui jumlah karakter dalam kata sandi.

Penulis telah menyajikan sebuah pendekatan yang dapat dilakukan untuk mengamankan data Administrasi rekam medis melalui Penggunaan QR Code Berbasis Kriptografi dengan metode AES Advanced Encryption Standard. Penulis berharap penelitian ini akan berkontribusi pada analisis yang lebih mendalam tentang QR code ini. Untuk penelitian lebih lanjut, penulis menyarankan untuk menambahkan waktu kedaluwarsa yang cepat pada QR Code untuk meningkatkan keamanan.

REFERENSI

[1] I. A. Ilyas dan S. Widodo, "Kriptografi File Menggunakan Metode Aes Dual Password," *Pros. Semin. Ilm. Nas. Komput. dan Sist. Intelijen (KOMMIT 2014)*, vol. 8, no. 2302–3740, hal. 263–270, 2014.

[2] M. Keabsahan, D. Krs, dan D. A. N. Khs, "Skripsi fatich fazlur rochman," 2016.

[3] E. Febriyanto, U. Rahardja, A. Faturahman, dan N. Lutfiani, "Sistem Verifikasi Sertifikat Menggunakan Qrcode pada Central Event Information," *Techno.Com*, vol. 18, no. 1, hal. 50–63, 2019, doi: 10.33633/tc.v18i1.2078.

[4] W. S. Agustina, R. Wajhillah, dan J. M. Hudin, "Penerapan Teknik Labeling QR Code Berbasis Intranet Pada Sistem Informasi Manajemen Aset RSUD. R. Syamsudin, SH. Sukabumi," *J. SWABUMI, Vol.5 No.2 Sept. 2017*, vol. 5, no. 2, hal. 181–190, 2017.

[5] A. T. Arief, W. Wirawan, dan Y. K. Suprapto, "Authentication of Printed Document Using Quick Response (QR) Code," *Proc. - 2019 Int. Semin. Intell. Technol. Its Appl. ISITIA 2019*, hal. 228–233, 2019, doi: 10.1109/ISITIA.2019.8937084.

[6] A. Suprianto dan A. A. F. Matsea, "Rancang Bangun Aplikasi Pendaftaran Pasien Online Dan Pemeriksaan Dokter Di Klinik Pengobatan Berbasis Web," *J. Rekayasa Inf.*, vol. 7, no. 1, hal. 48–58, 2018.

[7] A. K. Modern, "Standar Enkripsi Data."

[8] Y. W. Ti, S. K. Chen, dan W. C. Wu, "A New Visual Cryptography-Based QR Code System for Medication Administration," *Mob. Inf. Syst.*, vol. 2020, 2020, doi: 10.1155/2020/8885242.

[9] C. O. Mawalim, "Algoritma QR Code Digital Signature dengan Memanfaatkan Fingerprint," *Makal. IF4020 Kriptografi - Sem. II Tahun 2015/2016*, no. 13513031, 2016.

[10] R. 2011 Primartha, "Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)," *J. Res. Comput. Sci. Appl. Informatics Eng. Dep. Sriwij. Univ.*, vol. 01, no. 01, hal. 1–19, 2011.

[11] N. A. M. S. M. Mohamad Ali Murtadho, "Implementasi Quick Response (Qr) Code Pada Aplikasi Validasi Dokumen Menggunakan Perancangan Unified Modelling Language (Uml)," *Antivirus J. Ilm. Tek. Inform.*, vol. 10, no. 1, hal. 42–50, 2016, doi: 10.35457/antivirus.v10i1.87.

[12] A. Sulistyo, *Model Sistem Electronic Voting (E-Voting) Berbasis Web Dengan Menerapkan Quick Response Code (Qr-Code) Sebagai Sistem Keamanan Dalam Pemilihan Legislatif*. 2017.

[13] A. Manori, N. Devnath, N. Pasi, dan V. Kumar, "QR Code Based Smart Attendance System," *Int. J. Smart Bus. Technol.*, vol. 5, no. 1, hal. 1–10, 2017, doi: 10.21742/ijsbt.2017.5.1.01.

[14] T. Yuniati dan M. F. Sidiq, "Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital sebagai Alternatif Pengesahan Dokumen di Masa Pandemi," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 6, 2020, doi: 10.29207/resti.v4i6.2502.

[15] P. C. Huang, C. C. Chang, Y. H. Li, dan Y. Liu, "Efficient QR Code Secret Embedding Mechanism Based on Hamming Code," *IEEE Access*, vol. 8, hal. 86706–86714, 2020, doi: 10.1109/ACCESS.2020.2992694.

[16] D. V. S. Y. Sakti, N. Agani, dan M. Hardjianto, "Pengamanan Sistem Menggunakan One Time Password Dengan Pembangkit Password Hash SHA-256 dan Pseudo Random Number Generator (PRNG) Linear Congruential Generator (LCG) di Perangkat Berbasis Android," *J. Budi Luhur*, vol. 13, no. 1, hal. 1–3, 2016.

[17] V. Susukailo dan Y. Lakh, "Access control system based on encryption in QR-Code technology," *Proc. 2018 IEEE 4th Int. Symp. Wirel. Syst. within Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. IDAACS-SWS 2018*, hal. 158–161, 2018, doi: 10.1109/IDAACS-SWS.2018.8525779.

[18] С. В. Басенко dan Л. Е. Зеленков, "Сергей В. Басенко 1 *, Лев Е. Зеленков 1 1," vol. 51, no. 3, hal. 295–298, 2015.

[19] R. Munir, "Review Beberapa Block Cipher dan Stream Cipher Latar Belakang."

[20] E. T. E. H. A. El-Zain dan F. M. A. A. Ali, "Secure data using quick response code," *Proc. Int. Conf. Comput. Control. Electr. Electron. Eng. 2019, ICCCEEE 2019*, 2019, doi: 10.1109/ICCCEEE46830.2019.9070980.

[21] Okfalisa, N. Yanti, W. A. D. Surya, A. Akhyar, dan A. A. Frica, "Implementation of Advanced Encryption Standard (AES) and QR Code Algorithm on Digital Legalization System," *E3S Web Conf.*, vol. 73, hal. 1–7, 2018, doi: 10.1051/e3sconf/20187313009.

[22] Y. Zhan, "Anti-fake technology of commodity by using QR code," *Proc. - 2020 Int. Conf. E-Commerce Internet Technol. ECIT 2020*, hal. 1–4, 2020, doi: 10.1109/ECIT50008.2020.00008.