

PENGGUNAAN *QR CODE* BERBASIS KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES) UNTUK ADMINISTRASI REKAM MEDIS

Ferdiansyah

Universitas Jenderal Achmad Yani (UNJANI) Jawa Barat, Indonesia

Email: ferdiansyah@student.unjani.ac.id

INFO ARTIKEL

Diterima
25 September 2021
Direvisi
05 Oktober 2021
Disetujui
15 Oktober 2021

Kata Kunci:

kriptografi;
advanced encryption standard; *qr code*;
validasi

ABSTRAK

Data Administrasi dalam kesehatan dapat mengandung beberapa informasi penting, seperti identitas pasien, dokter, bahkan fasilitas kesehatan. Keamanan 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 dibagikan Dokumen untuk Manajemen Administrasi. Pada penelitian ini, pesan data Informasi rahasia disematkan ke *QR Code* berbasis Kriptografi dengan menggunakan Metode *Advanced Encryption 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 Encryption Standard* ini memberikan keuntungan dalam penggunaan yang mudah dan penggunaan sumber daya yang efisien.

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

How to cite:

Ferdiansyah (2021) Penggunaan Qr Code Berbasis Kriptografi Advanced Encryption Standard (AES) untuk Administrasi Rekam Medis. *Jurnal Syntax Admiration* 2 (10). <https://doi.org/10.46799/jsa.v2i10.325>

E-ISSN:

2722-5356

Published by:

Ridwan Institute

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;
 Code; validation*

QR

Pendahuluan

QR Code mampu menyimpan semua jenis data, seperti data angka/numerik, alpanumerik, biner (Widayati, 2017) (Febriyanto, Rahardja, Faturahman, & Lutfiani, 2019). 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 menyisipkan suatu objek pengenal seperti ID, atau tanda tangan yang digunakan untuk mencocokkan konten yang tertulis pada dokumen, yang kemudian akan disisipkan dan diproses sedemikian rupa menjadi sebuah kode yang akan diidentifikasi dan dicocokkan (Mohamad Ali Murtadho, 2016) *QR Code* merupakan teknik yang mengubah data tertulis menjadi kode 2 dimensi yang tercetak kedalam suatu media yang lebih ringkas (Huang, Chang, Li, & Liu, 2020). Dengan *QR Code*, informasi keaslian dokumen tersebut dibuat menjadi lebih sederhana dan simpel tanpa mengetikkan informasi kode atau surat keterangan pada dokumen tersebut (Belnye, 2018). Pada bidang Kesehatan, Potensi teknologi informasi telah berperan penting dan senantiasa mengalami modernisasi (Gunawan, Lim, Kartiwi, Malik, & Ismail, 2018) Hal ini dapat dilihat dari adanya akses luas dalam hal memperoleh informasi yang dibutuhkan dengan mudah (Widayati, 2017). Dengan adanya Sistem dalam bidang khususnya Kesehatan, Perubahan fungsi mulai bergeser pada sebuah kebutuhan dan Kerahasiaan terhadap data Administrasi (Rahmawati & Rahman, 2011).

Dibutuhkan sebuah cara yang dapat menjaga kerahasiaan dan keamanan pada perlindungan informasi dari pihak yang tidak sah. Salah satu mekanisme untuk meningkatkan keamanan data adalah dengan menggunakan teknik kriptografi. Kriptografi salah satunya adalah Algoritma *Advanced Encryption Standard* (Prasetyo & Suryana, 2016), data yang disimpan ke dalam *QR Code* kemudian disisipkan ke dokumen sehingga tidak mudah dibaca (Salleh, Saud, Nur, & Asnur, 2018). 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 didenkripsi menjadi bisa dibaca kembali (Ilyas & Widodo, 2014).

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 Terdapat beberapa kasus kebocoran data yang pernah terjadi di dunia. Salah satunya adalah yang terjadi pada perusahaan penyedia pencarian Sistem bernama *Just Dial* 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 (Rahmawati & Rahman, 2011). Kejadian ini disebabkan oleh Sistem Informasi yang masih menggunakan Aplikasi *RFID Radio Frequency Identity* (Susukailo & Lakh, 2018) 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*, (Febriyanto et al., 2019). 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* (Ti, Chen, & Wu, 2020) ada penelitian sebelumnya membahas tentang legalisasi ijazah dengan kriptografi visual untuk enkripsi dan dekripsi pada *RFID Code* dengan metode *DES Data Encryption Standard* tersebut (Zhan, 2020).

Penelitian-penelitian tersebut masih jarang dan hampir sudah tidak ada tentang penelitian *Data Encryption Standard* ini yang menerapkan keamanan yang baik terhadap Penggunaan metode tersebut (El-Zain & Ali, 2019).

Kemudian Penulis melakukan *Pembaruan* 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. 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 Advanced Encryption Standard* digunakan untuk mengamankan Teknik Enkripsi dan Dekripsi antara Fasilitas Kesehatan Klinik dengan Bagian Apoteker (Басенко & Зеленков, 2015). 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. Hasil dari penelitian ini akan bermanfaat dalam pengamanan data Administrasi, khususnya data yang bersifat rahasia seperti data Administrasi Rekam Medis.

Metode Penelitian

Tahapan penelitian yang akan dilakukan dalam penelitian ini terdiri dari Metode Kuantitatif dari lima tahapan yaitu; 1) Perolehan Data. 2) Spesifikasi Kebutuhan. 3). Perancangan dan Pembuatan Sistem 4) Implementasi 5) Pengujian.

Berikut merupakan tahapan penelitian ini:

a. Perolehan Data

Tahapan ini dilakukan terhadap perangkat lunak perolehan data secara umum Rekam Medis meliputi analisis masalah struktur Rekam Medis yang ditemukan pada perangkat lunak.

b. Spesifikasi Kebutuhan

Spesifikasi Kebutuhan, Kebutuhan sistem otentikasi kata sandi, *Library QR Code* Sistem ini berisikan algoritma yang berfungsi untuk memvalidasi pengguna dan Kata sandi untuk hak akses yang digunakan untuk mengakses data Administrasi rekam medis.

c. Perancangan dan Pembuatan Sistem *QR Code*

Sistem Aplikasi *QR Code*. proses penggabungan antara dokumen data Administrasi dengan *QR Code*. Pada tahap ini data Administrasi rekam medis, Data yang diambil untuk proses ini yaitu data berisi data Nomor Rekam Medis, Nama Pemeriksa, Jenis Kelamin, Jenis Pelayanan, Nama Pasien, Obat Utama, Keluhan, Tanggal Pemeriksaan, Diagnosa, Status Keluar, Biaya. Data-data tersebut adalah data yang tersedia pada data Administrasi Rekam medis. Jika terdapat data yang tidak ada pada salah satu data tersebut, maka data tersebut tidak akan digunakan pada proses validasi. Kemudian, pada tahap ini juga terdapat Spesifikasi Kebutuhan *QR Code*, Spesifikasi Perancangan Basis data, Spesifikasi Kebutuhan lainnya, Perancangan Diagram dan Aplikasinya dan Spesifikasi metode *AES Advanced Encyrption Standard* untuk Keamanan Sistem yang dibangun.

d. Implementasi

Implementasi *QR Code*, *QR Code* dibuat agar user dapat mengambil data rekam medis. *QR Code* ini berfungsi sebagai jalur komunikasi antara user dengan *QR Code* agar user dapat melakukan data Administrasi. *QR Code* ini juga berfungsi sebagai tempat untuk menyembunyikan dokumen dari data data Administrasi rekam medis.

e. Pengujian

pengujian. Pengujian perlu dilakukan untuk memastikan Sistem Aplikasi *QR Code* dengan metode *AES Advanced Encryption Standard* yang dibuat sudah sesuai dan aman. Maka Pengujian yang dilakukan adalah pengujian keamanan menggunakan *brute force*.

Hasil dan Pembahasan

Perancangan sistem 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.

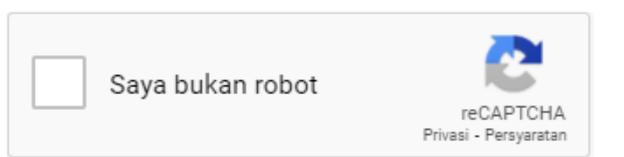
A. Perolehan Data

Pengumpulan Data yang diperoleh dari Fasilitas Kesehatan (Faskes) akan dikumpulkan 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
(google dev) Layanan *Captcha*

Tabel 3
Library *QR Code* (*phplib*)

Library <i>QR Code</i>
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*

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 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 = "6LcRo7QbAAAAAGUxiqlFSqIyGjR0hMBIRuRH3ugi";  
<div class="form-group">  
  <div class="g-recaptcha"  
    $data-sitekey="6LcRo7QbAAAAAI6ePvxTerTjOZ2cgpQm3V-ynExK">  
    <script src="https://www.google.com/recaptcha/api.js"></script>
```

D. Implementasi Dan Pengujian

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 *id admin username*, *password*, nama lengkap Tabel Admin dapat dilihat pada Gambar 3.

#	Nama	Jenis	Penyortiran	Tak			Komentar	Ekstra	Tindakan
				Atribut	Ternilai	Bawaan			
<input type="checkbox"/> 1	idadmin	int(5)			Tidak	Tidak ada	AUTO_INCREMENT	Ubah Hapus	
<input type="checkbox"/> 2	username	text	utf8_general_ci		Tidak	Tidak ada		Ubah Hapus	
<input type="checkbox"/> 3	password	text	utf8_general_ci		Tidak	Tidak ada		Ubah Hapus	
<input type="checkbox"/> 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
<input type="checkbox"/> 1	id	int(10)			Tidak	Tidak ada	AUTO_INCREMENT			Ubah Hapus Lainnya
<input type="checkbox"/> 2	no_reg	varchar(10)	utf8_general_ci	Ya		NULL				Ubah Hapus Lainnya
<input type="checkbox"/> 3	dokter	varchar(40)	utf8_general_ci	Ya		NULL				Ubah Hapus Lainnya
<input type="checkbox"/> 4	jns_kelamin	varchar(40)	utf8_general_ci	Ya		NULL				Ubah Hapus Lainnya
<input type="checkbox"/> 5	jns_layanan	varchar(40)	utf8_general_ci	Ya		NULL				Ubah Hapus Lainnya
<input type="checkbox"/> 6	pasien	varchar(40)	utf8_general_ci	Tidak		Tidak ada				Ubah Hapus Lainnya
<input type="checkbox"/> 7	jns_obat	varchar(40)	utf8_general_ci	Tidak		Tidak ada				Ubah Hapus Lainnya
<input type="checkbox"/> 8	kd_obat	varchar(40)	utf8_general_ci	Tidak		Tidak ada				Ubah Hapus Lainnya
<input type="checkbox"/> 9	tgl_periksa	date			Tidak	Tidak ada				Ubah Hapus Lainnya
<input type="checkbox"/> 10	diagnosa	varchar(40)	utf8_general_ci	Tidak		Tidak ada				Ubah Hapus Lainnya
<input type="checkbox"/> 11	status_byr	varchar(40)	utf8_general_ci	Tidak		Tidak ada				Ubah Hapus Lainnya
<input type="checkbox"/> 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.

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

Gambar 5
Tabel Data Obat

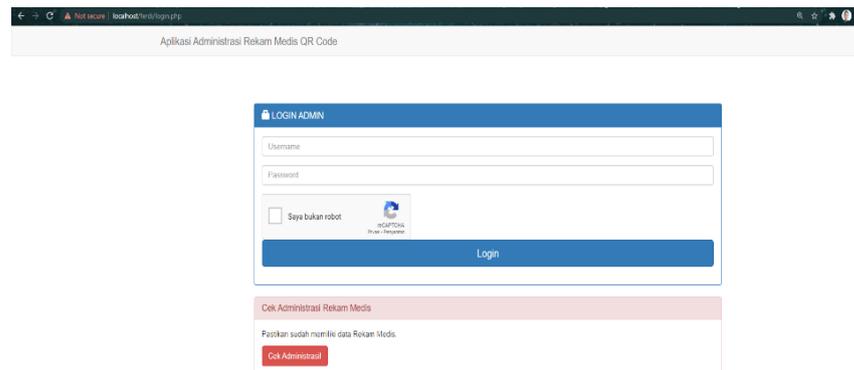
b) Implementasi Keamanan Aplikasi *QR Code*

Implementasi Aplikasi *QR Code* ini dilakukan berdasarkan perancangan yang telah dilakukan. Aplikasi *QR Code* ini mengimplementasikan *QR Code* dan mengirimkan datanya dalam format dokumen. dengan bahasa pemrograman *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 diamankan 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 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.

Penggunaan Qr Code Berbasis Kriptografi *Advanced Encryption Standard (AES)* untuk Administrasi Rekam Medis

Apikasi Rekam Medis QR Code Home Rekam Medis Data Obat Cek Validasi

Tambah Data Rekam Medis

Kode Rekam Medis

Nama Pemeriksa

Jenis Kelamin

Jenis Layanan

Nama Pasien

Jenis Obat

Keluhan

Tanggal Pemeriksaan

Diagnosa

Status Keluar

Biaya

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.

Apikasi Administrasi Obat QR Code Dokter Obat Cek Validasi Logout

Tambah Data Obat

Kode Registrasi Obat

Nama Obat

Jenis Obat

Kuantitas

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 10
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 *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 Encryption 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*.

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.

Penggunaan Qr Code Berbasis Kriptografi *Advanced Encryption Standard (AES)* untuk Administrasi Rekam Medis

Request	Payload	Status	Error	Timeout	Length
656	13b73edae8443990be1aa8f1a...	401	<input type="checkbox"/>	<input type="checkbox"/>	462
657	b497dd1a701a33026f72115336...	401	<input type="checkbox"/>	<input type="checkbox"/>	462
658	166ee015c0e0934a8781e0c86a...	401	<input type="checkbox"/>	<input type="checkbox"/>	462
659	7516c3b35580b3490248629cff5...	200	<input type="checkbox"/>	<input type="checkbox"/>	1430
660	701fb90716e10ecc7a43852e0ea...	401	<input type="checkbox"/>	<input type="checkbox"/>	462
661	061fba5bdfc076bb7362616668...	401	<input type="checkbox"/>	<input type="checkbox"/>	462
662	1c63129ae9db9c60c3e8aa94d3...	401	<input type="checkbox"/>	<input type="checkbox"/>	462

```
Request Response
Pretty Raw Render \n Actions
1 HTTP/1.1 200 OK
2 Date: Tue, 15 Jun 2021 13:20:51 GMT
3 Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.4.18
4 X-Powered-By: PHP/7.4.18
5 Access-Control-Allow-Origin: *
6 Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type
7 Access-Control-Allow-Methods: GET
8 Content-Length: 1027
9 Connection: close
```

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.

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 *Ciphertex* dan *Key* tersebut bisa dilakukan proses dekrip, artinya pada hasil pengujian ini bisa dilakukan telah dibuktikan metode *Advance Encryption Standard* ini layak untuk dipakai beberapa tahun ke depan, seperti yang dilihat pada gambar 12.

```
Word: localhost/login.php/ferdi/bruteaes
Password: admin
Key: b'8c697ce5b5416415bde988bd4dee15dfb167a9c873fc4b8ba81f6f2ab448a918'
Cipher: b'14637389c6ba2c53bae6e8d6cb635dbb433cdf329414c625282e7c13c7e4d545861b278f61133fbb49a58661af78dd6'
=====Bruce Force=====
```

Gambar 12
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 perangkat lunak telah memenuhi kebutuhan fungsional yang telah ditetapkan pada tahap sebelumnya.

Kesimpulan

Dari optimalisasi perangkat lunak hasil Implementasi di atas, maka bisa didapatkan 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 Encryption 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.

BIBLIOGRAFI

- Belnye, S. (2018). Branding and Identity. *Basics Interior Design 01: Retail Design*, 10–33. <https://doi.org/10.5040/9782940476107.0005>. [Google Scholar](#)
- El-Zain, E. T. E. H. A., & Ali, F. M. A. A. (2019). *Secure data using quick response code. Proceedings of the International Conference on Computer, Control, Electrical, and Electronics Engineering 2019, ICCCEEE 2019*. <https://doi.org/10.1109/ICCCEEE46830.2019.9070980>. [Google Scholar](#)
- Febriyanto, E., Rahardja, U., Faturahman, A., & Lutfiani, N. (2019). Sistem Verifikasi Sertifikat Menggunakan *Qrcode* pada *Central Event Information*. *Techno.Com*, 18 (1), 50–63. <https://doi.org/10.33633/tc.v18i1.2078>. [Google Scholar](#)
- Gunawan, T. S., Lim, M. K., Kartiwi, M., Malik, N. A., & Ismail, N. (2018). *Penetration testing using Kali linux: SQL injection, XSS, wordpres, and WPA2 attacks. Indonesian Journal of Electrical Engineering and Computer Science*, 12 (2), 729–737. <https://doi.org/10.11591/ijeecs.v12.i2.pp729-737>. [Google Scholar](#)
- Huang, P. C., Chang, C. C., Li, Y. H., & Liu, Y. (2020). *Efficient QR Code Secret Embedding Mechanism Based on Hamming Code*. *IEEE Access*, 8, 86706–86714. <https://doi.org/10.1109/Access.2020.2992694>. [Google Scholar](#)
- Ilyas, I. A., & Widodo, S. (2014). Kriptografi File Menggunakan Metode Aes Dual Password. *Prosiding Seminar Ilmiah Nasional Komputer dan Sistem Intelijen (Kommit 2014)*, 8 (2302–3740), 263–270. [Google Scholar](#)
- Mohamad Ali Murtadho, N. A. M. S. M. (2016). Implementasi *Quick Response (Qr) Code* Pada Aplikasi Validasi Dokumen Menggunakan Perancangan *Unified Modelling Language (Uml)*. *Antivirus: Jurnal Ilmiah Teknik Informatika*, 10 (1), 42–50. <https://doi.org/10.35457/antivirus.v10i1.87>. [Google Scholar](#)
- Prasetyo, R., & Suryana, A. (2016). Aplikasi Pengamanan Data dengan Teknik Algoritma Kriptografi *AES* dan Fungsi *Hash SHA-1* Berbasis Desktop. *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, 5 (2), 61. <https://doi.org/10.32736/sisfokom.v5i2.40>. [Google Scholar](#)
- Rahmawati, A., & Rahman, A. (2011). Sistem Pengamanan Keaslian Ijasah Menggunakan *QR-Code* dan Algoritma. *Seminar*, 1 (2), 105–112. [Google Scholar](#)
- Salleh, N., Saud, S., Nur, M., & Asnur, A. (2018). Pemanfaatan *QR-Code* sebagai media pembelajaran Bahasa Asing pada Perguruan Tinggi di Indonesia. *Seminar Nasional Dies Natalis UNM Ke 57*, (July), 253–260. Diambil dari <http://eprints.unm.ac.id/11298/>. [Google Scholar](#)

- Susukailo, V., & Lakh, Y. (2018). *Access control system based on encryption in QR-Code technology. Proceedings of the 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS-SWS 2018*, 158–161. <https://doi.org/10.1109/IDAACS-SWS.2018.8525779>. [Google Scholar](#)
- Ti, Y. W., Chen, S. K., & Wu, W. C. (2020). *A New Visual Cryptography-Based QR Code System for Medication Administration. Mobile Information Systems*, 2020. <https://doi.org/10.1155/2020/8885242>. [Google Scholar](#)
- Widayati, Y. T. (2017). *Aplikasi Teknologi Qr (Quick Response) Code Implementasi Yang Universal. Komputaki*, 3 (1), 66–82. [Google Scholar](#)
- Zhan, Y. (2020). *Anti-fake technology of commodity by using QR code. Proceedings - 2020 International Conference on E-Commerce and Internet Technology, ECIT 2020*, 1–4. <https://doi.org/10.1109/ECIT50008.2020.00008>. [Google Scholar](#)
- Басенко, С. В., & Зеленков, Л. Е. (2015). *Сергей В. Басенко 1 *, Лев Е. Зеленков 1* 1. 51 (3), 295–298. [Google Scholar](#)

Copyright holder:

Ferdiansyah (2021)

First publication right:

Jurnal Syntax Admiration

This article is licensed under:

