JSAI : Journal Scientific and Applied Informatics
Vol. 06, No. 02, Juni 2023, hal. 125~134
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085

Implementasi Algoritma *Base64* Pada *Transfer* Data *JSON* Rekam Medis Puskesmas Kembangseri Menggunakan *CURL*

[1]Ahmad Leo Napoleon, [2]M.Husni Rifqo
[1,2]Universitas Muhammadiyah Bengkulu, Indonesia
[3]Universitas Komputer Indonesia, Indonesia
[1]*Ahmadleo4525@gmail.com*; [2]*mhrifqo@umb.ac.id*;

Article Info

Article history:

Received, 2023-05-12
Revised, 2023-05-23
Accepted, 2023-05-31

Kata Kunci:

Enkripsi,
Kriptografi,
Rekam Medis,
JSON,
CURL

ABSTRAK

Puskesmas merupakan salah satu fasilitas kesehatan yang disediakan oleh pemerintah untuk masyarakat. Sebagai instansi yang bergerak dibidang kesehatan, dalam pengelolaan data rekam medis banyak yang menggunakan rekam medis elektronik. Dalam proses pengiriman serta penerimaan data belakangan ini data format *JSON* sering digunakan karena memiliki *resource* yang sedikit dibandingkan dengan format pertukaran data lainnya serta memanfaatkan *project open source CURL* sebagai konektivitas transfer data. Namun, dalam proses pengiriman data, belum banyak upaya pengamanan data tersebut. Surfshark sebuah perusahaan siber merilis sebuah laporan bahwa Indonesia menempati peringkat ketiga sebagai negara dengan jumlah kebocoran data terbanyak di dunia. Pada kuartal III tahun 2022, tercatat sebanyak 12,74 juta insiden kebocoran data di Indonesia hingga tanggal 13 September 2022. Perusahaan *Salt Security* yang juga merilis sebuah laporan bahwa ditemukan bahwa sebanyak 91% responden mengalami insiden keamanan API pada tahun 2020. Insiden tersebut mencapai tingkat tertinggi dan sebagian besar disebabkan oleh kerentanan (54%) dan masalah otentikasi (46%). Insiden lainnya meliputi boot/scraping (20%) dan serangan penolakan layanan atau denial of service (19%). Dampak dari kerentanan ini dapat menyebabkan kebocoran data, penyalahgunaan akun, atau adanya waktu henti pada layanan itu sendiri. Hal ini sangat disayangkan ditengah banyak nya perkembangan metode pengamanan data yang tidak dimanfaatkan sehingga menimbulkan kerugian bagi pemilik informasi. Metode pengamanan data dapat diterapkan sebagai upaya preventif meminimalisir resiko terhadap insiden kebocoran data. Metode yang diterapkan dalam pengembangan sistem ini adalah metode *prototipe*., algoritma yang digunakan untuk metode pengamanan adalah *Base64* dan untuk objek data yang digunakan dalam penelitian ini terdiri dari format data *JSON* yang berupa string. Setelah melaksanakan penelitian ini dan melewati proses pengujian *whitebox*, disimpulkan bahwa algoritma *Base64* dapat diimplementasikan pada format *JSON* yang bertipe *string*. Berdasarkan hasil uji whitebox yang dilakukan, tidak ditemukan adanya masalah atau kendala, dan sistem berhasil menghasilkan hasil yang sesuai dengan yang diinginkan. Oleh karena itu, penulis menyimpulkan bahwa sistem telah mencapai indeks keberhasilan 100%.

Keywords:

Encryption,
Cryptography,
Medical Records,
JSON,
CURL

ABSTRACT

Puskesmas is one of the health facilities provided by the government for the community. As an agency engaged in the health sector, many medical record data management uses electronic medical records. In the process of sending and receiving data, JSON format data is often used because it has few resources compared to other data exchange formats and utilizes the CURL open source project as data transfer connectivity. However, in the process of sending data, there has not been much effort to secure the data. Surfshark, a cyber company, released a report that Indonesia ranked third as the country with the highest number of data leaks in the world. In the third quarter of 2022, there were 12.74 million data leakage incidents in Indonesia until September 13, 2022. The Salt Security company also released a report that found that 91% of respondents experienced API security incidents in 2020. The incidents reached the highest level and were mostly caused by vulnerabilities (54%) and authentication issues (46%). Other incidents include boot/scraping (20%) and denial of service attacks (19%). The impact of these vulnerabilities can lead to data leakage, account abuse, or downtime in the service itself. This is unfortunate in the midst of many developments in data security methods that are not utilized, causing losses to information owners. Data security methods

JSAI : Journal Scientific and Applied Informatics
Vol. 06, No. 02, Juni 2023, hal. 125~134
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085

can be applied as a preventive effort to minimize the risk of data leakage incidents. The method applied in the development of this system is the prototype method, the algorithm used for the security method is Base64 and for the data object used in this study consists of JSON data format in the form of strings. After carrying out this research and passing the whitebox testing process, it is concluded that the Base64 algorithm can be implemented on JSON format of string type. Based on the whitebox test results, no problems or obstacles were found, and the system successfully produced the desired results. Therefore, the author concludes that the system has achieved a 100% success index.

Penulis Korespondensi:

Ahmad Leo Napoleon
Program Studi Informatika,
Universitas Muhammadiyah Bengkulu,
Email: Ahmadleo4525@gmail.com

1. PENDAHULUAN

Seiring dengan pesatnya perkembangan teknologi informasi, informasi telah menjadi kebutuhan pokok setiap orang. Informasi juga bagian penting bagi bisnis atau lembaga pemerintah, karena informasi dapat membantu bisnis untuk terus berkembang dalam persaingan global dan memfasilitasi penggunaan layanan publik untuk sektor pemerintahan. Permasalahan yang muncul dalam proses pengiriman atau penerimaan informasi adalah ketika informasi tersebut bersifat rahasia. Jika informasi tersebar luas melalui penyadapan, pencurian informasi, dan pemalsuan, maka akan merugikan pemilik informasi tersebut.

Dalam fasilitas pelayanan, terutama fasilitas kesehatan, terdapat sebuah dokumen penting yang disebut rekam medis. Rekam medis ini berfungsi sebagai catatan dan dokumen yang mencakup informasi mengenai identitas pasien, hasil pemeriksaan, jenis pengobatan, tindakan medis, dan pelayanan lain yang diberikan kepada pasien di fasilitas pelayanan kesehatan.

Dalam era penyebaran informasi yang cepat dan mudah diakses, keamanan informasi menjadi sangat penting. Untuk mengatasi hal tersebut, berbagai metode keamanan informasi telah ditingkatkan, salah satunya adalah dengan mengamankan pesan melalui pengubahan isi pesan agar tidak dapat dipahami oleh orang lain. Salah satu cara untuk menjaga keamanan dan kerahasiaan data atau informasi adalah dengan menggunakan teknik enkripsi dan dekripsi. Dengan menggunakan teknik ini, pesan atau data akan diubah sedemikian rupa sehingga tidak ada informasi yang bisa dibaca atau dipahami oleh pihak lain, kecuali oleh penerima yang sah.

Kriptografi merupakan kombinasi seni dan ilmu yang bertujuan untuk menghasilkan pesan yang rahasia. Proses ini melibatkan konversi pesan asli yang disebut *plaintext* menjadi pesan yang terenkripsi yang disebut *ciphertext* melalui proses enkripsi. Selanjutnya, *ciphertext* tersebut dapat dikembalikan menjadi *plaintext* asli melalui proses dekripsi[1].

JSON (JavaScript Object Notation) merupakan sebuah format pertukaran data yang memiliki keunggulan ringan, mudah dibaca dan ditulis oleh manusia, serta mudah diterjemahkan dan dibuat oleh komputer. Format ini didasarkan pada bagian dari bahasa pemrograman JavaScript, khususnya Standar ECMA-262 Edisi ke-3 yang diterbitkan pada bulan Desember 1990[2].

JSON berisi kumpulan pasangan kunci dan nilai (*key-value pairs*). Sintaksis *JSON* sangat sederhana dan jelas jika dibandingkan dengan format pertukaran data lainnya. *JSON* juga dapat digunakan dalam berbagai bahasa pemrograman, di mana setiap bahasa pemrograman memiliki metode interaksi yang unik dengan *JSON*[3]. Penulisan format *JSON* tidak bergantung pada bahasa pemrograman apapun, sehingga *JSON* dapat digunakan sebagai bahasa *transfer* data antar bahasa pemrograman. Struktur data universal digunakan pada *JSON*, meliputi kumpulan pasangan nilai atau objek (*object*) dan daftar nilai terurutkan atau larik (*array*)[9]. *JSON* adalah format data yang independen bahasa namun menggunakan konvensi penulisan yang akrab bagi para programmer yang berpengalaman dengan keluarga bahasa *C*, seperti *C, C++, C#, Java, JavaScript, Perl, Python* dan sebagainya. Sifat ini membuat *JSON* menjadi pilihan yang sangat baik sebagai bahasa untuk mengirim data[10].

cURL (*Client Uniform Resource Locator*) sebuah alat baris perintah yang memanfaatkan sintaks URL (*Uniform Resource Locator*) untuk mengirim dan menerima data, dan memiliki beragam fitur. hampir semua jenis perangkat yang terhubung dengan internet dan melakukan pertukaran data melalui internet menggunakan *cURL* sebagai alat untuk saling mengirim dan menerima data. *cURL* mendukung berbagai fitur, termasuk *FTP/FTPS, HTTP/HTTPS, IMAP, LDAP, POP3* dan lain-lain. Pada dasarnya, *cURL* adalah sebuah pustaka (*library*) yang

digunakan untuk mentransfer informasi. Dengan menggunakan pustaka ini, kode sumber halaman web dapat diambil sepenuhnya. *cURL* berfungsi sebagai alat komunikasi yang memungkinkan interaksi dengan berbagai jenis server dan protokol yang berbeda. Dengan bantuan cURL, pengguna dapat melakukan pengiriman dan pengambilan data melalui protokol-protokol yang didukung[11].

Salt Security, sebuah perusahaan keamanan API yang berbasis di Amerika Serikat, baru-baru ini meluncurkan laporan keamanan API mereka yang berjudul "*The State of API Security - Q1 2021*". Dalam rangka membuat laporan ini, perusahaan tersebut mengumpulkan data dari pelanggan mereka yang anonim serta tanggapan dari sekitar 200 profesional di bidang keamanan, aplikasi, dan *DevOps* melalui survei.

Menurut laporan tersebut, ditemukan bahwa sebanyak 91% responden mengalami insiden keamanan API pada tahun 2020. Insiden tersebut mencapai tingkat tertinggi dan sebagian besar disebabkan oleh kerentanan (54%) dan masalah otentikasi (46%). Insiden lainnya meliputi boot/scraping (20%) dan serangan penolakan layanan atau denial of service (19%). Dampak dari kerentanan ini dapat menyebabkan kebocoran data, penyalahgunaan akun, atau adanya waktu henti pada layanan itu sendiri.

Menurut perusahaan keamanan siber Surfshark yang juga merilis sebuah laporan bahwa Indonesia menempati peringkat ketiga sebagai negara dengan jumlah kebocoran data terbanyak di dunia. Pada kuartal III tahun 2022, tercatat sebanyak 12,74 juta insiden kebocoran data di Indonesia hingga tanggal 13 September 2022. Keamanan data merupakan aspek yang sangat penting dalam proses pengiriman informasi dan teks. Ada beberapa aspek yang harus diperhatikan untuk memastikan keaslian dan keamanan informasi, yaitu kerahasiaan (confidentiality), integritas (integrity), autentikasi (authentication), ketersediaan (availability), dan non-repudiation.

Minimnya sistem pengamanan pada proses penyebaran informasi mulai dari pengiriman hingga ke penerimaan data atau informasi pada instansi pelayanan kesehatan ini beresiko mengundang berbagai macam kejahatan dunia digital. Seperti pasien yang terjangkit virus Covid-19, HIV/AIDS dan berbagai penyakit yang dapat berpotensi merusak privasi dari pasien tersebut. Oleh karena itu, dibutuhkan suatu sistem keamanan pada format data yang dapat digunakan untuk mengantisipasi, serta menjaga kerahasiaan suatu data teks maupun informasi.

Berdasarkan uraian sebelumnya, dapat disimpulkan bahwa dalam penggunaan format *JSON*, sistem tersebut perlu dijamin keamanannya agar tidak mudah terbaca atau dipahami secara langsung oleh pihak yang tidak berwenang saat terjadi serangan *middle fight*, seperti pemalsuan data (*data forgery*) dan pelanggaran privasi (*Infringements of Privacy*). Hal ini bertujuan untuk melindungi kerahasiaan dan integritas data selama proses pertukaran, serta mencegah akses oleh pihak yang tidak berhak. Solusi yang dapat diterapkan adalah Teknik kriptografi sebagai pengamanan data. Berdasarkan hasil riset terdahulu yang menyatakan bahwa algoritma *Base64* memiliki proses yang sederhana dan cepat, namun dinilai efektif sebagai metode pengamanan, serta menghasilkan *chipertext* yang susah diketahui oleh orang awam, maka penulis memilih algoritma *Base64* sebagai metode pengamanan pada penelitian ini.

Dalam penelitian ini, penulis sedikit banyak mengambil referensi dari penelitian-penelitian sebelumnya yang berkaitan dengan topik pada penelitian ini. Terdapat beberapan penelitian terkait dengan algoritma enkripsi *Base64* dan implementasinya dalam segala bidang.

Pada penelitian pertama ini memiliki tujuan untuk memproteksi file video, sehingga menghasilkan sebuah kesimpulan bahwa "Algoritma *Base64* tersebut efektif karena base64 memiliki proses yang sederhana dan cepat namun aman, sehingga cara ini bisa dijadikan acuan untuk memproteksi file video"[4].

Penelitian kedua yang berkaitan selanjutnya memiliki tujuan mengamankan gambar yang terdiri dari susunan piksel yang kemudian dienkripsi, sehingga menghasilkan sebuah kesimpulan "Pengimplementasian algoritma base64 dan RC4 pada enkripsi gambar telah berhasil dibuat. Aplikasi yang dibangun tersebut dapat melakukan enkripsi dan dekripsi dengan baik. Aplikasi ini dibuat dengan Bahasa pemrograman web"[5].

Penelitian ketiga memiliki tujuan mengamankan presensi perkuliahan, sehingga menghasilkan sebuah kesimpulan "Berhasil menerapkan enkripsi *Base 64* dan *hasing SHA1* dan *MD5* sehingga terbentuk kode *QR* yang hasil uraian isinya lebih aman karena terenkripsi dan menjadi tulisan yang berisi kode yang tidak dapat langsung dimengerti oleh manusia"[6].

Penelitian keempat memiliki tujuan mengamankan teks sms, sehingga menghasilkan sebuah kesimpulan "Proses pengamanan pesan SMS menggunakan algoritma Base64 dapat berjalan dengan baik dan menghasilkan *ciphertext* yang susah diketahui oleh orang awam. Serta sistem keamanan pesan tergantung kepada kunci yang digunakan, pada penelitian ini kunci yang digunakan dalam string dan penulis menambahkan fungsi *hashing* yang merupakan bagian *library* kriptografi dari *class cryptography Java* "[7].

Keamanan adalah aspek yang sangat penting untuk suatu data atau informasi, dimana pengiriman data atau informasi membutuhkan keamanan yang tinggi untuk menghindari berbagaimacam kejahatan dalam dunia digital. Era modern ini kriptografi didefinisikan sebagai ilmu yang mengandalkan teknik matematika untuk menangani keamanan informasi seperti kerahasiaan, integritas data, dan otentikasi entitas untuk menghindari kejahatan tersebut[3].

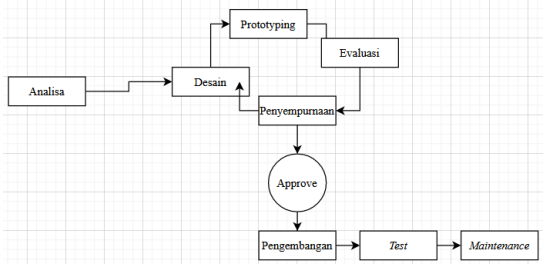
Keamanan informasi memiliki beberapa aspek yang harus dipenuhi untuk menjamin keaslian dan keamanan informasi. Aspek ini meliputi:

1. *Confidentiality*
   Aspek ini adalah aspek keamanan sistem sehingga orang yang tidak berwenang untuk mengakses informasi tidak dapat mengakses informasi tentang informasi penting dan rahasia.
2. *Integrity*
   Aspek ini menekankan bahwa informasi tidak diperbolehkan dimodifikasi tanpa persetujuan pemilik data. Untuk menjaga integritas data dengan tetap menjaga keaslian data yang dikirimkan, peneliti menerapkan teknik enkripsi pada data penting dan rahasia.
3. *Availability*
   Adalah mengacu pada ketersediaan informasi pada saat informasi dibutuhkan. Dalam hal ini, harus dapat menjamin bahwa pengguna informasi yang sah selalu dapat mengakses informasi dan sumber daya mereka sendiri. Untuk memastikan bahwa pengguna adalah orang yang benar-benar berhak mengakses informasi tersebut, hal ini dilakukan dengan menambahkan kata sandi pada informasi penting dan rahasia.

Enkripsi *base64* banyak digunakan di dunia internet sebagai media format data untuk pengiriman data, karena hasil pengkodean *base64* berupa teks biasa, sehingga data ini lebih mudah dikirim dibandingkan dengan data dalam bentuk biner. Karakter yang dihasilkan dari enkripsi Base64 ini terdiri dari A..Z, a..z dan 0..9 dengan penambahan simbol "+" dan "/" serta tanda sama dengan (=) pada dua karakter terakhir yang digunakan untuk mengisi pad, untuk mengadaptasi dan melengkapi data biner[12].
Kriptografi transformasi base64 banyak digunakan di dunia Internet sebagai media data format untuk mengirimkan data, penggunaan tersebut dikarenakan hasil dari encode base64 berupa plaintext, maka data ini akan jauh lebih mudah dikirim, dibandingkan dengan format data yang berupa binary. Algoritma base64 menggunakan kode ASCII dan kode index base64 dalam melakukan proses enkripsi ataupun dekripsinya[13].
Untuk pengamanan objek yang digunakan adalah format *JSON* yang berisi *key and value* dari *database MySQL.*SQL (Structured Query Language) adalah bahasa scripting untuk memproses database. *Database* besar seperti *MySQL*, *PostgreSQL* dan *SQL Server* sudah menggunakan *SQL* untuk memproses *database* mereka. Pengguna *MySQL* ini mempermudah dalam penyimpanan data (*backup*) di perusahaan[14]. *MySQL* mampu untuk melakukan banyak eksekusi perintah *query* dalam satu permintaan (*multithread*), baik itu menerima dan mengirimkan data[15]. *MySQL* menjadi pilihan utama dalam pengembangan web dan aplikasi berbasis web, dikarenakan *MySQL* dapat memproses jutaan permintaan dan ribuan transaksi sekaligus[16].
Aplikasi yang dibangun menggunakan *PHP*. Fungsi dari tag *PHP* adalah untuk mendefinisikan isi dalam file tersebut adalah sebuah dokumen[17]. Pada awalnya, *PHP* dirancang untuk diintegrasikan dengan web *server Apache*. Namun belakangan ini, *PHP* juga dapat bekerja dengan web *server* seperti *PWS* (*Personal Web Server*), *IIS* (*Internet Information Server*) dan Xitami. Yang membedakan *PHP* dengan bahasa pemrograman lain adalah adanya tag penentu, yaitu diawali dengan “<?” atau “<?php” dan diakhiri dengan “?>”. Jadi kita bebas menempatkan skrip *PHP* dimanapun dalam dokumen *HTML* yang telah kita buat[18].

2. METODE PENELITIAN

Metode yang digunakan pada penelitian ini adalah metode pengembangan sistem *prototype*. Pembuatan prototipe paradigma dimulai dengan mengumpulkan persyaratan. Pengembang dan klien bertemu dan menentukan tujuan keseluruhan dari perangkat lunak, mengidentifikasi persyaratan yang diketahui dan menguraikan area di mana definisi yang lebih rinci diperlukan, dan kemudian melakukan "desain *flash*".



Gambar 1 Metode Pengembangan Prototype

3. HASIL DAN PEMBAHASAN

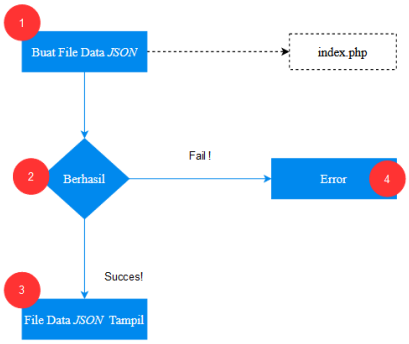
A. Hasil Implementasi

Setelah dilaksanakannya penelitian, diharapkan memperoleh hasil sesuai yang telah direncanakan sebelunya setelah melewati beberapa proses pengujian. Pada penelitian ini, penulis menerapkan proses pengujian *whitebox*. Sekenario pengujian dapat dilihat pada table dibawah ini :

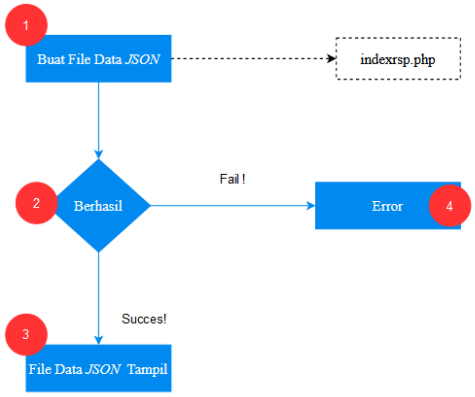
JSAI : Journal Scientific and Applied Informatics
Vol. 06, No. 02, Juni 2023, hal. 125~134
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085

Pengujian	Sekenario	Hasil Yang Diharapkan
Pembuatan File Data *JSON*	Membuat data *JSON* index.php menggunakan data yang berada di dalam *Database* 1 lalu mengenkripsinya.	Berhasil menampilkan data *JSON* index.php yang telah dienkripsi.
Pembuatan File Data *JSON Response*	Membuat data *JSON Response* indexrsp.php sebagai respon terhadap data *JSON* index.php kemudian mendeskripsinya	Berhasil menampilkan data *JSON* indexrsp.php yang telah dideskripsi.
Pembuatan File Input Data *JSON* Ke *Database* 2	*Insert* data *JSON Response* indexrsp.php sebagai respon terhada data *JSON* index.php	Berhasil *insert* data *JSON* indexrsp.php ke dalam *Database* 2

Tabel 1 Sekenario Pengujian Sistem



Gambar 2 Diagram Pengujian Pembuatan Data *JSON*



Gambar 3 Diagram Pengujian Pembuatan *Response JSON*

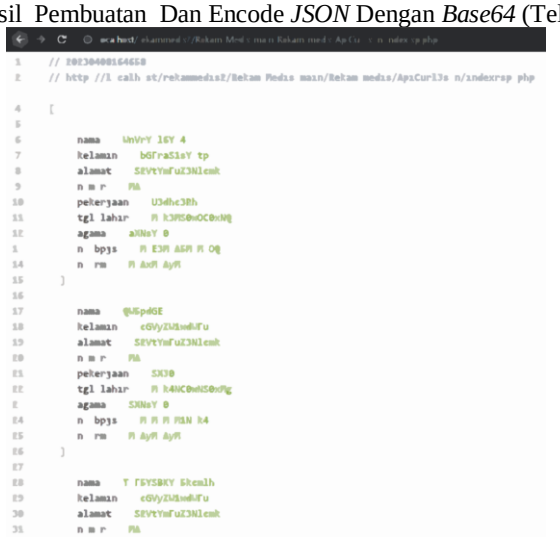
Setelah melaksanakan proses pengujian, ditemukan beberapa hasil. Berikut adalah tabel hasil dari pengujian sistem didukung dengan bukti pengujian pada objek data *JSON* :

Pengujian	Sekenario	Hasil Yang Diharapkan	Alur		Keterangan	
			1-2-3	1-2-4	Berhasil	Gagal
Pembuatan File Data *JSON*	Membuat data *JSON* index.php menggunakan data yang berada di dalam *Database* 1 lalu mengenkripsinya.	Berhasil menampilkan data *JSON* index.php yang telah dienkripsi.	✓		✓	
Pembuatan File Data *JSON Response*	Membuat data *JSON Response* indexrsp.php sebagai respon terhadap data *JSON* index.php kemudian mendeskripsinya	Berhasil menampilkan data *JSON* indexrsp.php yang telah dideskripsi.	✓		✓	
Pembuatan File Input Data *JSON* Ke *Database* 2	*Insert* data *JSON Response* indexrsp.php sebagai respon terhada data *JSON* index.php	Berhasil *insert* data *JSON* indexrsp.php ke dalam *Database* 2	✓		✓	

Tabel 2 Hasil Sekenario Pengujian Sistem *Whitebox*

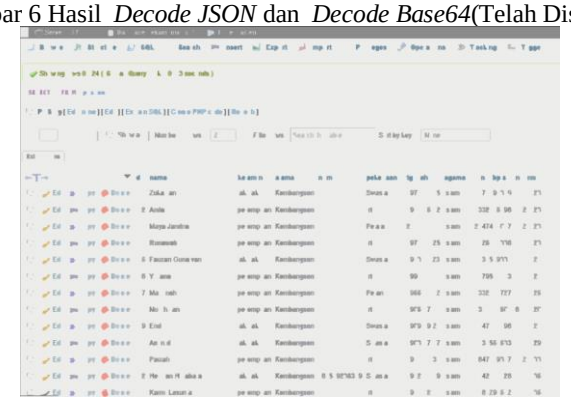
JSAI : Journal Scientific and Applied Informatics
Vol. 06, No. 02, Juni 2023, hal. 125~134
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085

Gambar 4 Hasil Pembuatan Dan Encode *JSON* Dengan *Base64* (Telah Disensor)



Gambar 5 Hasil Pembuatan *Response JSON*(Telah Disensor)

Gambar 6 Hasil *Decode JSON* dan *Decode Base64*(Telah Disensor)



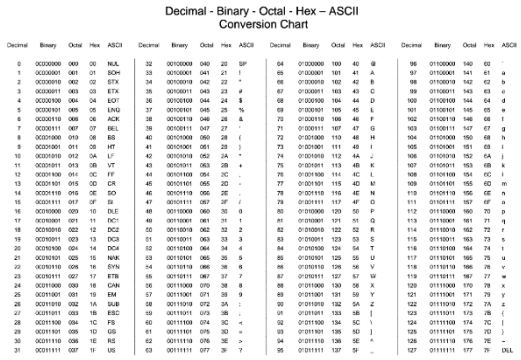
Gambar 7 Hasil *Insert* Data *JSON* ke *Database 2*(Telah Disensor)

B. PEMBAHASAN

1. Perhitungan Manual *Base64*

Proses perhitungan manual dari *Base64* dilakukan dengan cara mengubah karakter asli kedalam angka *decimal* dan 8bit *binary* menggunakan tabel *ASCII*, setelah itu deretkan 8bit *binary* tersebut dan kelompokkan menjadi 6bit *binary*. Jika terdapat bilangan bit *binary* yang tidak tercukupi maka harus di genapkan dengan nilai 0 hingga tercukupi menjadi 6bit *binary* dan setiap nilai 00 dari hasil penggenapan tersebut bernilai 1 *padding* atau =, setelah itu konversikan 6bit *binary* tersebut kedalam nilai *index* yang dimiliki *base64*. Setiap hasil enkripsi dari *base64* yang mengandung *padding*, dapat dipastikan bahwa jumlah karakter yang dienkripsi bukan bilangan kelipatan tiga sehingga menghasilkan *padding* disetiap hasil enkripsinya.

JSAI : Journal Scientific and Applied Informatics
Vol. 06, No. 02, Juni 2023, hal. 125~134
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085



Gambar 8 Konversi *Decimal-Binary ASCII*

Value	*Encoding*	*Value*	*Encoding*	*Value*	*Encoding*	*Value*	*Encoding*
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	-
15	P	31	f	47	v	63	_
						(*pad*)	=

Tabel 3 Pengkodean *Base64*

Perhitungan Karakter “Islam”. Dapat dilakukan dengan menyelesaikan tahap berikut :

1) Konversikan karakter asli nya yaitu “Islam “ke dalam decimal dan 8 bit *binary* menggunakan tabel konversi *ASCII.*

Karakter	ASCII	
	Desimal	8 Bit Binary
I	73	01001001
s	115	01110011
l	108	01101100
a	97	01100001
m	109	01101101

Tabel 4 Hasil Konversi *ASCII*

2) Kemudian deretkan angka 8 bit *binary* menjadi 6 bit *binary* seperti dibawah ini

Plaintext	I	s	l	a	m		
8Bit Binary	01001001	01110011	00111000	01101100	01101101		
6Bit Binari	010010	010111	001101	101100	011000	010110	1101 00

Tabel 5 Hasil Konversi 8Bit *Binary*-6Bit *Binary*

3) Maka langkah terakhir adalah menkonversi angka 6 bit *binary* ke decimal dan karakter yang dimiliki *base64*

6Bit Binari	010010	010111	001101	101100	011000	010110	1101 00
Desimal	18	23	13	44	24	22	52
Karakter	S	X	N	s	Y	W	0 =

Tabel 6 Hasil Konversi 6Bit *Binary-Base64*

Maka hasil enkripsi dari karakter “Islam” yang merupakan *value* dari data *JSON* menggunakan *Base64* adalah”SXNsYW0=”.

Untuk proses *decode* manual dari *base64*, kita hanya mengembalikan tahap dari proses *encode* nya dengan memanfaatkan *base64_decode*();, maka karakter yang sudah di *encode* sebelumnya akan kembali ke *plaintext.*

4. KESIMPULAN

Setelah menyelesaikan tahap pengimplementasian dan tahap pengujian *whitebox* terhadap format data *JSON* rekam medis, tidak ditemukan kendala sehingga dapat disimpulkan bahwa : algoritma *Base64* dapat digunakan untuk metode pengamanan data *JSON* yang bertipe *string* . Penelitian ini berjalan sesuai dengan yang direncanakan serta memperoleh hasil seperti yang diharapkan sehingga memiliki indeks keberhasilan 100%. Berdasarkan hasil dari implementasi, penulis menyarankan bahwa penelitian ini bisa dikembangkan dengan

mengkombinasikan dengan algoritma kriptografi lainnya sebagai metode pengamanan dan meningkatkan nya ke tahap enkripsi.

REFERENSI

[1] Yusfrizal, "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 29–37, 2019.

[2] M. G. L. Putra and M. I. A. Putera, "Analisis Perbandingan Metode Soap Dan Rest Yang Digunakan Pada Framework Flask Untuk Membangun Web Service," *SCAN - J. Teknol. Inf. dan Komun.*, vol. 14, no. 2, pp. 1–7, 2019, doi: 10.33005/scan.v14i2.1480.

[3] M. Firman Arif and M. Misdram, "Implementasi Enkripsi Url Pada Website Menggunakan Metode Base64 Dan Rotation13," *Spirit*, vol. 12, no. 1, pp. 20–25, 2020, [Online]. Available: http://jurnal.stmik-yadika.ac.id/index.php/spirit/article/view/166

[4] S. Supiyandi, H. Hermansyah, and K. A. P. Sembiring, "Implementasi dan Penggunaan Algoritma Base64 dalam Pengamanan File Video," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 340, 2020, doi: 10.30865/mib.v4i2.2042.

[5] M. Hayaty and M. D. Putra, "Enkripsi Dan Dekripsi Gambar Dengan Menggunakan Perpaduan Algoritma Base64 Dan Rc4," *Core It*, vol. 5, pp. 1–6, 2018, [Online]. Available: https://ojs.amikom.ac.id/index.php/semnasteknomedia/article/view/1986

[6] H. Witriyono and S. Fernandez, "Enkripsi Base 64, Hashing SHA1 dan MD5 pada QR Code Presensi Kuliah," *JSAI (Journal Sci. Appl. Informatics)*, vol. 4, no. 2, pp. 263–272, 2021, doi: 10.36085/jsai.v4i2.1680.

[7] R. Minarni, "Implementasi Algoritma Base64 untuk Mengamakan SMS pada Smartphone," *Build. Informatics, Technol. Sci.*, vol. 1, no. 1, pp. 28–33, 2019, [Online]. Available: http://ejurnal.seminar-id.com/index.php/bits/article/view/3

[9] R. Sahrial, D. F. Fauzi, and E. Susilawati, "Pemanfaatan Json Untuk Menampilkan Data Realtime Covid-19 Dengan Model View Presenter," *J. Teknoinfo*, vol. 16, no. 1, p. 144, 2022, doi: 10.33365/jti.v16i1.780.

[10] D. S. Wiyono and A. Wijayanto, "Implementasi Rest Web Service Dengan Menggunakan Json Pada Aplikasi Mobile Enterprise Resource Planning," *PERFORMA Media Ilm. Tek. Ind.*, vol. 11, no. 2, pp. 143–152, 2012.

[11] A. N. A. Zumaroh *et al.*, "Development of Application Programming Interface (Api) for Amikom Purwokerto Handsanitizer (Ampuh) Data Logger Visualization," *J. Tek. Inform.*, vol. 3, no. 3, pp. 791–796, 2022, [Online]. Available: http://jutif.if.unsoed.ac.id/index.php/jurnal/article/view/222

[12] I. Afrianto and N. Taliasih, "Sistem Keamanan Basis Data Klien P.T. Infokes Menggunakan Kriptografi Kombinasi RC4 Dan Base64," *J. Nas. Teknol. dan Sist. Inf.*, vol. 6, no. 1, pp. 9–18, 2020, doi: 10.25077/teknosi.v6i1.2020.9-18.

[13] E. Gunadhi and A. P. Nugraha, "Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection," *J. Algoritm.*, vol. 13, no. 2, pp. 391–398, 2017, doi: 10.33364/algoritma/v.13-2.391.

[14] T. Rahmasari, "Perancangan Sistem Informasi Akuntansi Persediaan Barang Dagang Pada Toserba Selamat Menggunakan Php Dan Mysql," *is Best Account. Inf. Syst. Inf. Technol. Bus. Enterp. this is link OJS us*, vol. 4, no. 1, pp. 411–425, 2019, doi: 10.34010/aisthebest.v4i1.1830.

[15] T. N. Putri, Rifnaldi, and Surmayanti, "Penggunaan Bahasa Pemrograman PHP Dan MySQL Sebagai Penunjang Sistem Informasi Persediaan Dan Penjualan Secara Online," *J. Pendidik. Teknol. Inf.*, vol. 5, no. 2, pp. 64–73, 2019, [Online]. Available: http://lppm.upiyptk.ac.id/ojsupi/index.php/pti Vol.

[16] K. Sidharta and T. Wibowo, "Studi Efisiensi Sumber Daya Terhadap Efektivitas Penggunaan Database : Studi Kasus Sql Server Dan Mysql," *Conf. Business, Soc. Sci. Innov. Technol.*, vol. 1, no. 1, pp. 508–515, 2020, [Online]. Available: http://journal.uib.ac.id/index.php/cbssit

[17] R. R. Fadila, W. Aprison, and H. A. Musril, "Perancangan Perizinan Santri Menggunakan Bahasa Pemograman PHP/MySQL Di SMP Nurul Ikhlas," *CSRID (Computer Sci. Res. Its Dev. Journal)*, vol. 11, no. 2, p. 84, 2021, doi: 10.22303/csrid.11.2.2019.84-95.

[18] A. Mubarak, "Rancang Bangun Aplikasi Web Sekolah Menggunakan Uml (Unified Modeling Language) Dan Bahasa Pemrograman Php (Php Hypertext Preprocessor) Berorientasi Objek," *JIKO (Jurnal Inform. dan Komputer)*, vol. 2, no. 1, pp. 19–25, 2019, doi: 10.33387/jiko.v2i1.1052.