

Pengamanan Database Sistem Pendaftaran Online Dengan Kriptografi Aes-256-Cbc Pada TK Islam Baitul Khoir

by Hari Soetanto

Submission date: 28-Aug-2023 09:27AM (UTC+0700)

Submission ID: 2152410069

File name: e_Dengan_Kriptografi_AES-256-CCBC_Pada_TK_Islam_Baitul_Khoir.pdf (1.21M)

Word count: 3183

Character count: 19579

PENGAMANAN DATABASE SISTEM PENDAFTARAN ONLINE DENGAN KRIPTOGRAFI AES-256-CBC PADA TK ISLAM BAITUL KHOIR

Rizky Putra Mahendra^{1*}, Hari Soetanto²

^{1, 2}Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email: ^{1*} rizkymahendra2346@gmail.com, ² hari.soetanto@budiluhur.ac.id
(*: corresponding author)

Abstrak-Di era yang serba digital saat ini, hampir semua orang melakukan pekerjaannya dibantu dengan internet. Dari pekerjaan yang besar hingga pekerjaan yang mudah dapat diselesaikan dengan menggunakan internet. Pendaftaran *online* merupakan salah satu pekerjaan yang dapat dilakukan secara daring, pendaftaran secara daring dapat membantu proses pendaftaran agar dapat dilakukan dimana saja dan kapan saja. TK Islam Baitul Khoir merupakan lembaga pendidikan jenjang taman kanak-kanak dan masih melakukan pendaftaran secara *offline*, sistem pendaftaran *online* ini akan dirancang untuk dapat mengenkripsi data berupa *file* data *text* yang *diinput* oleh *user*. Terlepas dari itu keamanan data menjadi sangat penting untuk diamankan agar pihak yang tidak berwenang tidak dapat mengakses data pendaftaran yang sensitif. Cara yang tepat untuk mengamankan suatu data adalah menggunakan teknik kriptografi. Teknik kriptografi yaitu suatu teknik yang bertujuan untuk mengacak data menjadi data yang tidak dapat dibaca oleh manusia kecuali manusia yang memiliki akses berupa *key* pada data tersebut yang biasanya dimiliki oleh si pengirim dan si penerima data. Dalam penelitian ini menggunakan teknik algoritma kriptografi AES-256-CBC (*Advanced Encryption Standard 256 Cipher Block Chaining*) untuk mengamankan data yang bersifat rahasia. Lalu akan dilakukan pengujian proses enkripsi dan dekripsi untuk memastikan bahwa proses kriptografi berjalan dengan baik dan efisien. Dari hasil pengujian yang telah dilakukan, diketahui jumlah karakter hasil enkripsi bergantung pada jumlah karakter asli. Dan durasi proses kriptografi bergantung pada kecepatan *resource* yang digunakan berupa prosesor, ram dan internet. Kesimpulan akhir yang didapat dari penelitian ini adalah data para pendaftar menjadi lebih aman dari pihak yang tidak bertanggung jawab.

Kata Kunci: sistem pendaftaran online, AES-256-CBC, kriptografi

SECURING OF ONLINE REGISTRATION SYSTEM DATABASE WITH AES-256-CBC CRYPTOGRAPHY AT TK ISLAM BAITUL KHOIR

Abstract-In today's digital era, almost everyone does their work with the help of the internet. From big jobs to easy jobs can be completed using the internet. Online registration is one of the jobs that can be done online, online registration can help the registration process so that it can be done anywhere and anytime. Baitul Khoir Islamic Kindergarten is a kindergarten level educational institution and is still registering offline, this online registration system will be designed to be able to encrypt data in the form of text data files inputted by the user. Apart from that, data security is very important to be secured so that unauthorized parties cannot access sensitive registration data. The right way to secure data is to use cryptographic techniques. Cryptographic technique is a technique that aims to scramble data into data that cannot be read by humans unless humans have access in the form of a key to the data which is usually owned by the sender and recipient of the data. This research uses the AES-256-CBC (*Advanced Encryption Standard 256 Cipher Block Chaining*) cryptographic algorithm to secure confidential data. Then the encryption and decryption process will be tested to ensure that the cryptographic process runs well and efficiently. From the results of the tests that have been carried out, it is known that the number of characters from the encryption result depends on the number of original characters. And the duration of the cryptographic process depends on the speed of the resources used in the form of processors, RAM and the internet. The final conclusion obtained from this study is that the data of the registrants is safer from irresponsible parties.

Keywords: online registration system, AES-256-CBC, cryptography

1. PENDAHULUAN

Di era perkembangan teknologi yang sangat pesat ini hampir semua aspek memerlukan hal-hal yang berbau digital, ini dikarenakan teknologi mempermudah pekerjaan manusia dalam melakukan kegiatan yang dilakukannya, kebanyakan teknologi digital dapat melakukan pekerjaannya secara otomatis tanpa campur tangan manusia selain sebagai operator, karena pekerjaannya dilakukan secara otomatis sangat membantu mengurangi bahkan menggantikan pekerjaan yang dilakukan oleh manusia.

TK Islam Baitul Khoir adalah suatu yayasan yang berdiri pada bidang pendidikan di jenjang taman kanak-kanak dan tiap tahunnya pendaftar semakin meningkat, maka dari itu TK Islam Baitul Khoir membutuhkan sistem pendaftaran online yang dapat membantu dalam mengurus pekerjaan administrasi pendaftaran.

Sistem pendaftaran online bertujuan untuk mempermudah proses pendaftaran [1]. Sistem pendaftaran online ini dapat membantu orang tua pendaftar karena sistem tersebut diharapkan dapat memudahkan proses pendaftaran, dengan begitu pendaftar hanya perlu mengisi form pendaftaran secara online dengan keamanan yang tinggi karena setiap data yang dikirimkan akan dienkripsi terlebih dahulu sebelum disimpan ke dalam *database*.

Cryptography berasal dari bahasa Yunani, terdiri dari kata *crypto* dan *graphia* yang berarti 'penulisan rahasia'. Kriptografi adalah pengetahuan atau keterampilan mengamati dan mempelajari bagaimana merahasiakan pesan yang dikirim oleh pengirim agar dan memastikan bahwa pesan tersebut disampaikan secara rahasia kepada penerima. [2].

Kriptografi adalah sebuah metode yang tepat untuk menjaga keamanan suatu data yang bersifat sensitif, dalam kriptografi terdapat dua proses pengamanan yaitu proses enkripsi dan proses dekripsi, dalam enkripsi dan dekripsi data menggunakan kriptografi metode algoritma AES (*Advanced Encryption Standard*) diperlukan sebuah encryption key yang sama. Data yang dinilai sensitif akan di enkripsi dan dekripsi menggunakan metode algoritma AES (*Advanced Encryption Standard*) sebelum disimpan ke *database* atau *cloud storage*.

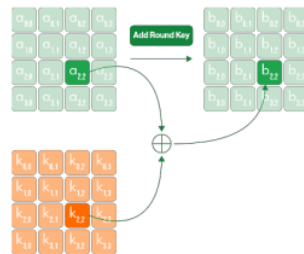
Algoritma AES merupakan algoritma enkripsi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang berbeda yaitu 10, 128, 192, dan 256 bit [3]. AES memiliki kecepatan enkripsi dan dekripsi tertinggi bersama *Blowfish*, DES, dan IDEA [4]. Algoritma kriptografi AES termasuk dalam kelas algoritma kriptografi kunci simetris dan kunci yang digunakan untuk enkripsi sama dengan kunci yang digunakan untuk dekripsi [5].

Dalam kriptografi modern, panjang kunci dalam ukuran jumlah bit yang digunakan, merupakan salah satu faktor yang sangat penting. Hal ini disebabkan karena penggunaan komputer yang sangat intensif dalam dunia kriptografi. *Advanced Encryption Standard* (AES) diperkenalkan pada tahun 1997. NIST telah mengumumkan bahwa AES akan menggantikan algoritma enkripsi Data Encryption Standard (DES) yang sudah ketinggalan zaman dan tidak aman. AES sekarang menjadi *block cipher* yang dapat memproses blok 256-bit dari *input* yang berupa *plaintext* dalam suatu waktu. AES juga telah mendukung pengaturan kunci 128, 192, dan 256-bit dan lebih efisien daripada DES. [6]

Hal yang pertama dilakukan dalam enkripsi algoritma AES adalah melakukan *input XOR plaintext/state* yang akan di enkripsi dengan *roundkey*, kemudian melakukan XOR *plaintext* dengan *roundkey*. Lalu melakukan substitusi dengan *S-Box*. Setelah itu hasil dari substitusi dengan *S-Box* selesai. Dilakukan *shiftrow*. Setelah hasil *shiftrow* didapat, kemudian langkah berikutnya adalah melakukan *Mix Columns* dengan mengalikan matrik. Setelah perhitungan *Mix Column* selesai kemudian dilakukan *addround key*. Yaitu melakukan XOR *state* dengan *round key*. Lakukan sampai iterasi 14, namun pada saat putaran/iterasi yang ke 14, setelah step *shiftrow* lompat step *Mix Columns* dan langsung lanjut melakukan XOR hasil *state* saat *shift row* dengan *round key*. [7]

a. *AddRoundKey*

Pada gambar 1 menunjukkan representasi dari proses *AddRoundKey*. Sebuah *round key* ditambahkan pada *state* dengan operasi XOR. Masing-masing *round key* terdiri dari N_b *word* di mana setiap *word* tersebut ditambahkan dengan *word* atau kolom yang sesuai dengan *state*.



Gambar 1. *AddRoundKey*

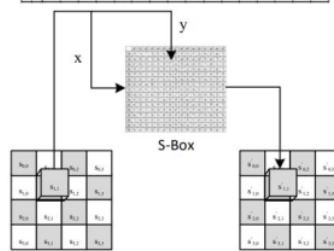
b. *SubBytes*

SubBytes adalah transformasi *byte* di mana setiap elemen pada *state* dipetakan dengan tabel substitusi (*S-Box*). Untuk setiap *byte* dalam *array state*, misalkan $S[r,c]=xy$, yang dalam hal ini xy adalah digit heksadesimal dari nilai $S[r,c]$, nilai substitusi dilambangkan $S[r,c]$, adalah elemen dari tabel substitusi yang menunjukkan pengaruh

pemetaan *byte* pada setiap *byte* dan *state*. Tabel 1 menunjukkan tabel *s-Box* dan gambar 2 menunjukkan ilustrasi transformasi *SubBytes*.

Tabel 1. *s-Box*

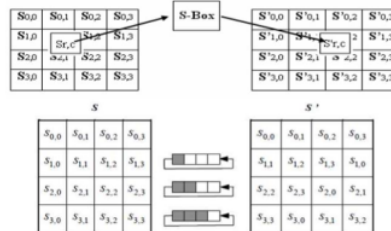
	y															
x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	42	6b	64	c5	30	01	67	2b	5e	d7	ab	76
1	ca	82	c9	7d	fa	59	47	80	ad	d4	a2	af	5c	a4	72	c0
2	b7	6d	93	26	3e	3f	e7	0c	34	a5	e5	f1	71	08	31	15
3	44	c7	23	c3	38	94	05	5a	07	12	89	e2	ab	27	32	75
4	09	83	2c	3a	0b	6a	5a	a0	52	3e	d6	53	29	a3	2f	84
5	53	d1	00	ed	10	fc	b1	5b	6a	cb	ba	39	4a	4c	58	cf
6	d0	ef	aa	eb	43	6d	33	85	45	f9	02	72	50	3c	9f	a8
7	51	a3	40	8f	32	9d	38	e5	bc	b6	da	21	10	ff	f3	d2
8	ed	0c	13	ac	1f	37	44	17	c4	a7	7a	36	64	5d	19	73
9	60	81	4e	6e	22	2a	90	88	4e	ee	39	14	da	5a	0b	db
a	e0	32	3a	6a	49	06	24	5c	c2	d3	ae	62	91	95	ed	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	aa	65	7a	ae	08
c	ba	78	25	2e	3c	a6	b4	c6	e8	d4	74	1f	4b	6b	0b	8a
d	70	3e	35	66	48	03	25	0e	41	35	37	39	86	c1	1d	9e
e	a1	f8	98	11	e9	d9	0a	34	9b	2a	87	a9	ca	55	28	d4
f	7e	a1	89	08	32	ed	42	58	41	99	2d	6e	30	34	bb	14



Gambar 2. *SubBytes*

c. *ShiftRows*

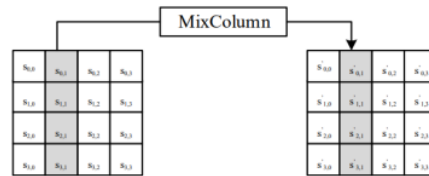
Gambar 3 menunjukkan ilustrasi *ShiftRows*. *ShiftRows* adalah proses yang melakukan pergeseran dalam elemen blok/tabel yang perlu dilakukan baris demi baris, baris pertama tidak perlu dilakukan pergeseran sebanyak 2 *byte* cukup geser baris ke-4 sebanyak 3 *byte*.



Gambar 3. *ShiftRows*

d. *MixColumn*

Transformasi *MixColumn()* dilakukan setelah transformasi *ShiftRows*, yaitu sumber utama propagasi untuk algoritma AES. Difusi merupakan prinsip pendistribusian efek dari *bit plaintext* atau kunci *bit* pada *ciphertext* sebanyak mungkin. Transformasi *MixColumn()* mengalikan setiap kolom dari *array state* dengan polinomial $a(x) \text{ mod } (x^4 + 1)$. Setiap kolom diperlakukan sebagai polinomial 4 suku pada GF (28). Ditunjukkan pada gambar 4 ilustrasi *MixColumn*.



Gambar 4. *MixColumn*

e. Proses Dekripsi

Proses dekripsi algoritma AES di mulai dengan meng-XOR *chipertext* dengan *AddRows* lalu lakukan *InvShiftRows* dan *InvSubByte* kemudian Tranformasi *InvMixColumns* sama dengan *MixColumns*, yang membedakannya yaitu $a(x)$ yang digunakan adalah *invers* nya (a^{-1}).

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam membangun sistem registrasi *online* pada TK Islam Baitul Khoir Dimulai dengan tahapan analisis kebutuhan data, perancangan algoritma, dan implementasi sistem (dalam hal ini menggunakan bahasa pemrograman JavaScript), dilanjutkan ke tahap pengujian sistem.

2.1 Analisa Sistem

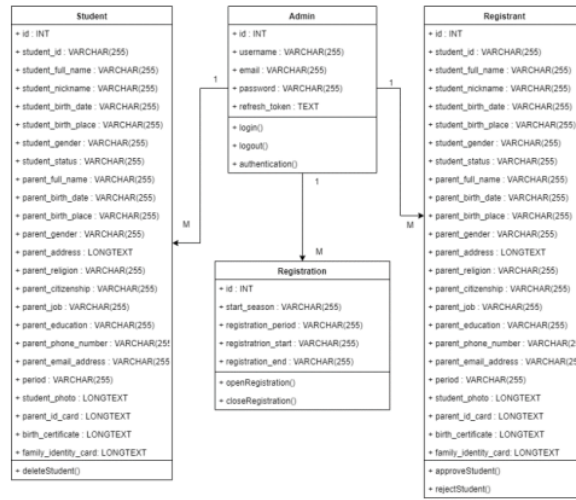
Berdasarkan kekurangan sistem registrasi *online* sebelumnya pada TK Islam Baitul Khoir, maka dari itu peneliti merancang sistem registrasi *online* yang baru untuk digunakan. Sistem yang akan dibangun menggunakan bahasa pemrograman Javascript dengan *frontend* menggunakan *library* Reactjs, sedangkan untuk *backend* menggunakan *library* Express dan *database* MySQL. Langkah pertama yang dilakukan adalah merancang kebutuhan basis data lalu membuat *user interface* yang menarik dan mudah untuk digunakan oleh pengguna.

2.2 Design (Pemodelan)

Menurut [8] pemodelan merupakan fase di mana proses dan data yang dibutuhkan oleh sistem baru ditentukan. Perancangan sistem ini merupakan gambaran menyeluruh dari alur pemrosesan data mulai dari pembuatan rancangan sistem hingga pembuatan laporan-laporan yang dibutuhkan.

2.3 Class Diagram

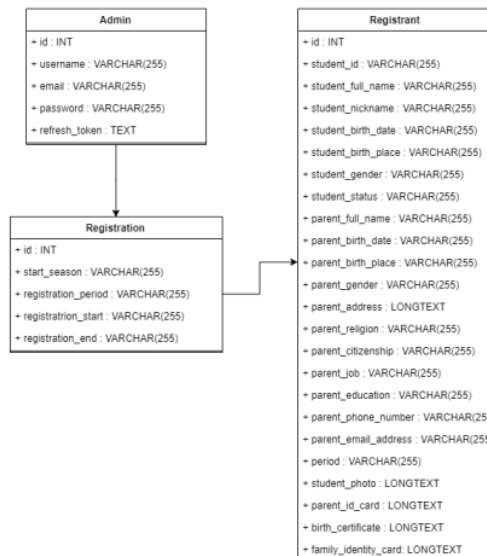
Menurut [9] *Class diagram* merupakan sebuah model yang menggambarkan struktur dan deskripsi *class* dan hubungannya antara *class* lain. *Class diagram* menggambarkan model yang digunakan untuk merancang atribut dan fungsi yang digunakan untuk membuat desain sistem baru. *Class diagram* sistem pendaftaran *online* ditunjukkan pada gambar 5.



Gambar 5. Class Diagram

2.4 Logical Record Structure (LRS)

LRS merupakan struktur *record* pada tabel yang terbentuk dari hasil di seluruh kumpulan entitas. Memiliki aturan dasar yang sangat dipengaruhi oleh faktor utama yang menarik perhatian. [10] *Logical Record Structure* pada sistem pendaftaran online dapat dilihat pada gambar 6.



Gambar 6. Logical Record Structure (LRS)

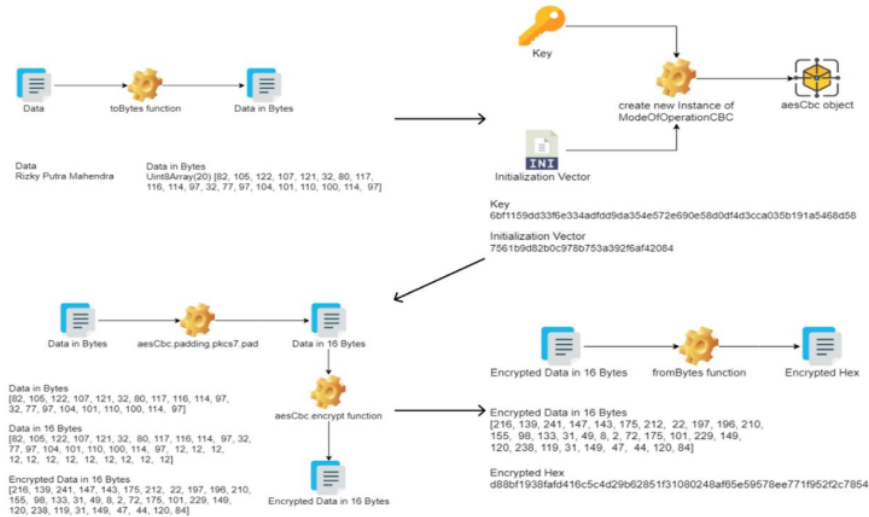
3. HASIL DAN PEMBAHASAN

3.1 Implementasi Metode

Pada sub bab ini menjelaskan penerapan metode kriptografi menggunakan algoritma *Advanced Encryption Standard 256 Cipher Block Chaining* (AES 256 CBC) yang dibantu menggunakan *library* Aes-js. Proses kriptografi dilakukan pada *backend*, data yang masuk melalui *form* registrasi dan keluar untuk ditampilkan pada *website dashboard* akan melalui proses kriptografi sehingga data yang disimpan pada *database* merupakan data yang sudah tidak dapat dibaca oleh manusia.

3.2 Proses Enkripsi

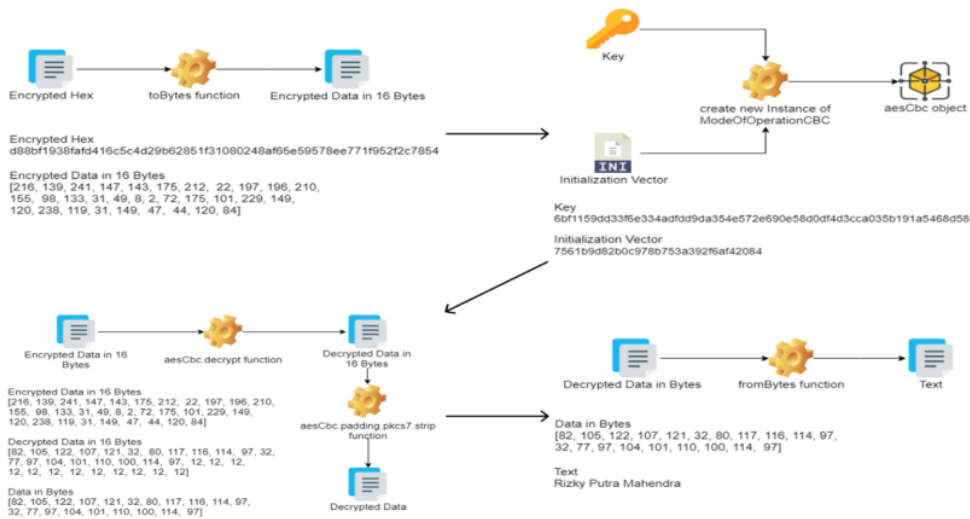
Hal pertama proses enkripsi yang dilakukan adalah mengubah plaintext menjadi *bytes* dengan kelipatan 16. Kemudian membuat *instance* baru dari Aes-js dengan memberikan parameter *key* dan *initialization vector* lalu akan menghasilkan *object* baru untuk digunakan pada langkah selanjutnya. Lalu mengenkripsi data dengan kelipatan 16 *bytes*, data terlebih dahulu melewati fungsi *pad* untuk memastikan bahwa data yang akan dienkripsi adalah *bytes* dengan kelipatan 16. Setelah data menjadi *bytes* dengan kelipatan 16 dienkripsi dengan menggunakan *method encrypt* dari *object* yang telah dibuat pada langkah sebelumnya. Langkah terakhir yaitu mengkonversi data kelipatan 16 *bytes* yang telah dienkripsi menjadi tipe data *hex*. Ilustrasi proses enkripsi sistem pendaftaran *online* dapat dilihat pada gambar 7.



Gambar 7. Proses enkripsi dengan library Aes-js

3.3 Proses Dekripsi

Tahap dekripsi pertama-tama mengubah hex yang ingin didekripsi menjadi bytes dengan kelipatan 16. Kemudian membuat *instance* baru dari Aes-js dengan memberikan parameter *key* dan *initialization vector* lalu akan menghasilkan *object* baru untuk digunakan pada langkah selanjutnya. Lalu mendekripsi data dengan kelipatan 16 *bytes* menggunakan *method* dari *object* yang telah dibuat pada langkah sebelumnya, data terlebih dahulu melewati fungsi *pad* untuk memastikan bahwa data yang akan didekripsi adalah *bytes* dengan kelipatan 16. Setelah data menjadi *bytes* dengan kelipatan 16 didekripsi dengan menggunakan *method decrypt* dari *object* yang telah dibuat pada langkah sebelumnya. Langkah terakhir yaitu mengkonversi data kelipatan 16 *bytes* yang telah didekripsi menjadi tipe data *hex*. Gambar 8 menunjukkan proses dekripsi sistem pendaftaran *online*.



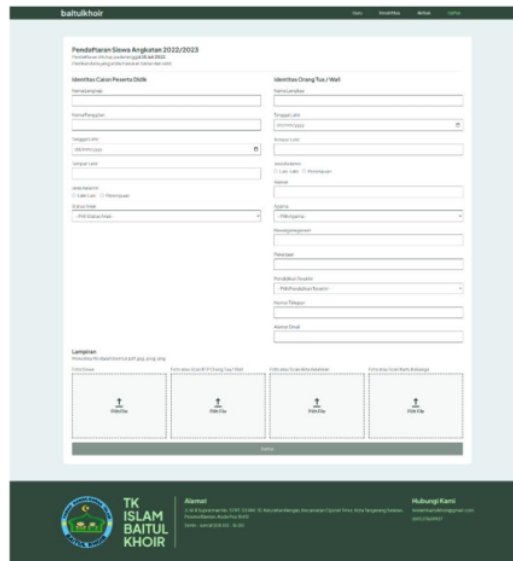
Gambar 8. Proses dekripsi dengan library Aes-js

3.4 Tampilan Layar

Hasil penerapan sistem registrasi *online* peserta didik baru pada TK Islam Baitul Khoir Tangerang Selatan yang bertujuan untuk mempermudah proses pendaftaran.

a. Tampilan Layar *Form* Pendaftaran

Gambar 9 menunjukkan tampilan layar dari halaman pendaftaran, pada halaman ini menampilkan formulir pendaftaran untuk para pendaftar untuk melakukan pendaftaran pada TK Islam Baitul Khoir. Setelah *user* mengisi formulir dan klik 'daftar' disini lah proses enkripsi berlangsung, setelah selesai enkripsi selesai data formulir disimpan ke dalam *database*.



Gambar 9. Halaman *form* pendaftaran pada *website* pendaftar

b. Tampilan Layar *Login Dashboard Admin*

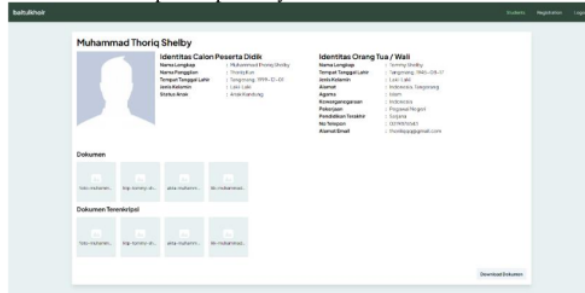
Berikut ini adalah tampilan layar dari halaman *login* yang ditunjukkan pada gambar 10, terdapat dua buah *input field* untuk memasukkan *username* dan *password* sebagai proses autentikasi.



Gambar 10. Halaman *login dashboard admin*

c. Tampilan Layar Detil Pendaftar

Gambar 11 dibawah merupakan tampilan layar dari halaman detil siswa, pada halaman ini berisi data siswa dengan lebih detil beserta dokumen pendukung yang terdaftar di TK Islam Baitul Khoir. Di bagian ini proses dekripsi berlangsung sebelum data ditampilkan pada layar.



Gambar 11. Tampilan layar detil pendaftar

3.5 Pengujian

Dari pengujian yang telah dilakukan dengan memfokuskan terhadap sisi kecepatan dan hasil enkripsi yang berupa banyak karakter dan berapa ukuran data sebelum dan sesudah dienkripsi menggunakan algoritma kriptografi AES-256-CBC (*Advanced Encryption Standard 256 Cipher Block Chaining*). Tabel 1 dan 2 dibawah ini menunjukkan hasil pengujian kriptografi yang dilakukan.

Tabel 2 Pengujian Kriptografi Data *String*

Karakter Asli	Hasil Enkripsi	Jumlah Karakter		Waktu	
		Asli	Enkripsi	Enkripsi	Dekripsi
Rizky Putra Mahendra	d88bf1938afd416c5c4d29b62851f31080248af65e59578ee771f952f2c7854	20	64	10.207 ms	7.365 ms
Rizky	78fbdde5231676d9fe978b2bdf4cc3a2	5	32	13.354 ms	40.585 ms
23-04-2000	0d858f768cfaa3c1ce83ae6a1b94219f	10	32	31.745 ms	15.598 ms
Jakarta	86217c22b49c4dc267aa345135a3f5d5	7	32	22.577 ms	9.694 ms
Laki-Laki	0493c0585aeb3a577c79d1228581b3fb	9	32	0.832 ms	8.73 ms

Anak Kandung	6a6005ee4840b9fd24e8540c9cb48eb4	12	32	14.376 ms	6.958 ms
Sullivan	e9b11cad293a54a7e72a1b23deee8cb9	8	32	36.824 ms	17.183 ms
17-08-1945	4e9dfdd9bd077318cae18f5e1525f5dc	10	32	15.776 ms	10.972 ms
Dublin	86217c22b49c4dc267aa345135a3f5d5	7	32	15.336 ms	10.511 ms
Laki-Laki	0493c0585aeb3a577c79d1228581b3fb	9	32	17.081 ms	8.73 ms
Indonesia, Jakarta	04b50becec52e31225280db58c836c1e5d52497b648e65cafe248a82122e4640	17	64	24.461 ms	8.086 ms
Islam	d52d10410f9a97b594ef3c908b3d15ef	5	32	15.293 ms	5.539 ms
Indonesia	faafd971811ef59e4a2da32c95f77b43	10	32	14.114 ms	7.386 ms
Pegawai Swasta	f816d71d45a145960fe3c91247221260	14	32	20.136 ms	7.818 ms
Sekolah Menengah Akhir Atau Sederajat	ad6f028fd965a9dd3e7f521c0ec5283461478b3907b9ac21f08f12032cf6116f4ed2c3a5d8cf850f08de66a0b3e14bf8	37	96	60.696 ms	10.659 ms
0212345678	242d69b9ac07373d94be62e960f9d955	10	32	184.996 ms	11.934 ms
sullivan@email.com	f29839871fd992d11a1b5888706034ef627688d1ed7f2a09078d513cf8683d57	18	32	97.512 ms	6.563 ms
2022/2023	a72ebbd02b109fe9bfa1ba578afe277	9	32	582.991 ms	9.308 ms

Tabel 3 Pengujian Kriptografi File

Nama File	Ukuran File		Waktu	
	Asli	Enkripsi	Enkripsi	Dekripsi
sample-photo.jpg	6.564 bytes	0 bytes	6.564 bytes	374.014 ms
sample-idcard.png	300.857 bytes	0 bytes	300.857 bytes	2.658 s
sample-birthcertificate.png	1.403.929 bytes	0 bytes	1.403.929 bytes	7.852 s
sample-kk.jpg	51.703 bytes	0 bytes	51.703 bytes	368.117 ms

Dari pengujian enkripsi pada tabel 1 dan tabel 2 diketahui bahwa kecepatan enkripsi dan dekripsi tidak selalu sama tergantung dengan *resource* spesifikasi *hardware* yang digunakan. Enkripsi data berupa *string* panjang karakter bertambah menjadi 32 hingga 64 tergantung dari panjang karakter aslinya, sementara pada enkripsi *file* perubahan ukuran file tidak dapat diketahui karena ketika proses *download file* yang terenkripsi dilakukan, sistem tidak dapat memproses *string* yang terenkripsi menjadi *file* sehingga menghasilkan *file* dengan ukuran 0 *byte* atau *file corrupt*.

4. KESIMPULAN

Setelah melakukan tahap perancangan dan pembuatan sistem kemudian dilanjutkan dengan tahap implementasi dan pengujian dapat disimpulkan bahwa sistem ini memudahkan pendaftar dan administrator TK Islam Baitul Khoir, Sistem ini berbasis *website* untuk administrator dan pendaftar yang dibuat menggunakan

library reactjs dan dengan adanya sistem registrasi *online* yang menggunakan keamanan AES-256-CBC (*Advanced Encryption Standard 256 Cipher Block Chaining*) dapat mengamankan data pendaftar.

DAFTAR PUSTAKA

- [1] N. A. Rumana, E. I. Apzari, D. R. Dewi, L. Indawati, dan N. Yulia, "Penerimaan Pasien Terhadap Sistem Pendaftaran Online Menggunakan Technology Acceptance Model di RSUP Fatmawati," *Faktor Exacta*, vol. 13, no. 1, p. 44, Jun. 2020, doi: 10.30998/faktorexacta.v13i1.5611.
- [2] R. Laia, "Implementasi Algoritma Aes 256 Bit Dan Lsb Untuk Pengamanan Dan Penyisipan Pesan Teks Pada File Audio," *Jurnal Pelita Informatika*, vol. 8, no. 4, pp. 467–469, 2020.
- [3] A. Prameshwari dan N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Informatika*, vol. 8, no. 1, p. 52, Sep. 2018, doi: 10.30864/eksplora.v8i1.139.
- [4] A. Puji Nugroho, H. Bayu Suseno, dan U. Islam Negeri Syarif Hidaytullah Jakarta, "Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES," *Jurnal Sistem Informasi*, 2020.
- [5] A. Kusyanti dan K. Amron, "Analisis Perbandingan Algoritma Advanced Encryption Standard Untuk Enkripsi Short Message Service (SMS) Pada Android," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 2, no. 10, pp. 4281–4289, 2018, [Online]. Available: <http://j-ptiik.ub.ac.id>
- [6] Mulyadi, "Aplikasi Kriptografi Pesan Teks Menggunakan Algoritma Advanced Encryption Standard 256 Bit," *Aplikasi Kriptografi Pesan Teks Menggunakan Algoritma Advanced Encryption Standard 256 Bit (AES-256) Dan Diffie Hellman*, vol. 3, 2019.
- [7] A. Pariddudin dan F. Syaqui, "Penerapan Algoritma AES pada QR CODE untuk Keamanan Verifikasi Tiket," vol. 10, pp. 43–52, 2020, doi: 10.36350/jbs.v10i2.
- [8] H. Sulistiani, L. Ratu, dan B. Lampung, "Penerapan Metode Cost And Benefit Analysis Dalam Pengukuran Investasi Teknologi Informasi," *Jurnal TEKNOKOMPAK*, vol. 14, no. 1, p. 54, 2020.
- [9] W. Alakel, I. Ahmad, dan E. Budi Santoso, "Sistem Informasi Akuntansi Persediaan Obat Metode First In First Out (Studi Kasus: Rumah Sakit Bhayangkara Polda Lampung)," 2019. doi: <https://doi.org/10.33365/jtk.v13i1.269>.
- [10] A. Taufik, "Perancangan Sistem Informasi Penjualan Makanan Kucing Dan Anjing Berbasis Web," *JUMIKA*, vol. 6, no. 2, 2019.

Pengamanan Database Sistem Pendaftaran Online Dengan Kriptografi Aes-256-Cbc Pada TK Islam Baitul Khoir

ORIGINALITY REPORT

11 %
SIMILARITY INDEX

%
INTERNET SOURCES

7 %
PUBLICATIONS

7 %
STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

4%

★ Submitted to Universitas Brawijaya

Student Paper

Exclude quotes On

Exclude matches < 1%

Exclude bibliography On