Volume 13 Number 2, July 2023 Page. 286-300
Journal Homepage: http://teknois.unbin.ac.id/index.php/JBS
DOI Link: http://doi.org/10.36350/jbs.v13i2

ISSN : 2087 - 3891 (PRINT)
ISSN : 2597 - 8918 (DIGITAL)
Jurnal Ilmiah Teknologi - Informasi & Sains
TEKNOIS
Universitas Binaniaga Indonesia
Change, Continuous Quality Improvement, De'bottlenecking, Enhancement... Do It!

Article DOI: 10.36350/jbs.v13i2.205
Received: May; Accepted: June; Published: July

Penerapan Algoritma AES 256 Pada Qr Code Untuk Sistem Registrasi Event Sepeda

Mohamad Dani Saputro[1], Binanda Wicaksana[2*], Farhan Zayid[3]
[1] Teknik Informatika/ Universitas Binaniaga Indonesia
Email: mohamaddanisaputro@gmail.com
[2] Teknologi Informasi/ Universitas Binaniaga Indonesia
Email: binandawicaksana@gmail.com
[3] Teknologi Informasi/ Universitas Binaniaga Indonesia
Email: farhan.zayid@gmail.com
) Corresponding Author

ABSTRACT

Technology and the digital era are currently developing rapidly and providing various conveniences for humans in various aspects, including in the field of event organizers. After the Covid-19 pandemic ended, events began to be held again in various areas, including in Bogor. Bicycle events are one of the events that are highly anticipated by bicycle hobbyists, but there are still many event organizers who depend on Google Forms as a place to register participants. The problems that occur in the registration system using the Google form are related to data management and the ineffectiveness and efficiency the registration process because according to the value the registration process used at this time is still quite convoluted, causing queues at the time of re-registration of participants. In addition, there is no security that can maintain the authenticity of participant data, because currently registration data that is input via Google Form is directly stored automatically on Google Drive where the Google Drive account can still be accessed together so that leaks and tracing errors will be difficult to do. Therefore, the application of the AES 256 algorithm to the QR code is considered the right solution to increase system effectiveness, efficiency and security. registration. This research has carried out a feasibility test on a prototype that was built based on the evaluation value of the system which has been carried out through a questionnaire by 2 experts and 5 users showing that the system developed is very feasible with a percentage value of 84%. Thus, the use of the AES 256 algorithm on the QR code can be declared effective and efficient for increasing participant data security in the mountain bike event registration system.

Keywords: *Information Technology, AES Algorithm, Registration System, Mountain Bike Event, data security, Cryptography, QR code*

ABSTRAK

Teknologi dan era digital saat ini berkembang pesat dan memberikan berbagai kemudahan bagi manusia dalam berbagai aspek, termasuk dalam bidang event organizer. Setelah pandemi Covid-19 berakhir, event-event mulai diadakan kembali di berbagai daerah, termasuk di Bogor. Event sepeda menjadi salah satu event yang sangat dinantikan oleh para penghobi sepeda, namun masih banyak pihak penyelenggara event yang bergantung pada Google Form sebagai tempat dilakukan pendaftaran peserta. Permasalahan yang terjadi pada sistem registrasi menggunakan google form ini adalah terkait pengelolaan data dan belum efektifnya serta efisiensi proses registrasi karena di nilai proses registrasi yang digunakan saat ini masih cukup berbelit belit sehingga menimbulkan antrian pada saat registrasi ulang peserta. Selain itu, belum adanya keamanan yang dapat menjaga keaslian data peserta, dikarenakan registrasi saat ini data yang di inputkan melalui Google Form

Volume 13 Number 2, July 2023 Page. 286-300
Journal Homepage: http://teknois.unbin.ac.id/index.php/JBS
DOI Link: http://doi.org/10.36350/jbs.v13i2

langsung tersimpan otomatis pada Google Drive dimana akun google drive masih dapat diakses bersama-sama sehingga memungkinkan terjadinya kebocoran serta tracing kesalahan akan sulit dilakukan. Oleh karena itu, penerapan algoritma AES 256 pada QR code dianggap sebagai solusi yang tepat untuk meningkatkan efektivitas, efisiensi, dan keamanan sistem registrasi. Penelitian ini sudah dilakukan uji kelayakan pada prototype yang dibangun berdasarkan nilai evaluasi sistem yang telah dilakukan melalui kuesioner oleh 2 ahli dan 5 pengguna menunjukkan bahwa sistem yang dikembangkan sangat layak dengan nilai presentase 84%. Dengan demikian, penggunaan algoritma AES 256 pada QR code dapat dinyatakan efektif dan efisien untuk meningkatkan keamanan data peserta pada sistem registrasi event sepeda gunung.

Kata kunci: *Teknologi Informasi, Algoritma AES, Sistem Registrasi, Event Sepeda Gunung, keamanan data, Kriptografi, QR code*

A. PENDAHULUAN

1. Latar belakang

Pasca pandemi COVID-19 berakhir, banyak event mulai digelar kembali di berbagai daerah, termasuk di Bogor. Sebagai kota tujuan wisata yang kaya akan kuliner dan rute rute yang menarik, Bogor sering menjadi tempat diadakannya event, termasuk event sepeda. Diperkirakan terdapat lebih dari 50 komunitas sepeda di Bogor yang tercatat di dalam Paguyuban Pesepeda Bogor Raya (PPBR), dengan masing-masing komunitas memiliki anggota sekitar 20-200 orang. Salah satu komunitas sepeda yang cukup besar di Bogor adalah Komunitas Sepeda Gunung Bogor (KSGB), dengan sekitar 100 anggota. Setelah pandemi COVID-19 berakhir, KSGB menjadi pelopor di kota Bogor dengan mengadakan event bertajuk "KSGB XC Team Marathon". Dalam rangka mematuhi protokol kesehatan dan aturan kapasitas yang berlaku, partisipasi dalam event ini dibatasi hanya untuk 31 komunitas yang terpilih.

Setelah pendaftaran ditutup, masih ada beberapa komunitas yang ingin bergabung dalam event tersebut, bahkan beberapa di antaranya berasal dari luar daerah. Namun, kehadiran mereka dianggap sebagai rombongan liar dan di luar kapasitas panitia penyelenggara event. Komunitas yang telah terdaftar harus melakukan registrasi pendaftaran dengan cepat melalui Google Form yang telah disebarkan oleh panitia melalui media sosial. Dalam waktu kurang dari seminggu, sudah ada lebih dari 30 komunitas yang terdaftar sehingga hanya komunitas terpilih yang dapat mengikuti event ini. Registrasi merupakan sebuah aktivitas proses pendaftaran yang harus dilalui untuk dapat mengikuti suatu program, kegiatan, atau menjadi anggota dari sebuah organisasi. Tujuan dari registrasi adalah untuk mengumpulkan informasi tentang orang yang terlibat, mencatat partisipasi mereka, dan menetapkan akses mereka ke dalam program atau organisasi yang bersangkutan. Namun, banyak kendala dan keterbatasan dalam proses registrasi menggunakan Google Form, seperti proses yang tidak efektif dan efisien, sehingga pengelolaan data terasa lebih lama, serta masalah keamanan data pribadi peserta mengingat data yang masuk ke dalam Google Form tersimpan langsung di Google Drive dimana akun Google Drive tersebut masih digunakan Bersama sama oleh panitia yang lain sehingga bisa saja melakukan kesalahan seperti ketidaktahuan menggunakan Google Drive yang menyebabkan salah klik dan ternyata data malah dibagikan kepada orang lain sehingga tracing kesalahan akan sulit dilakukan, Oleh karena itu, sangatlah penting menerapkan keamanan agar kualitas data dapat terjaga keasliannya.Untuk mengatasi kebutuhan tersebut, dibutuhkan sebuah sistem yang terintegrasi dengan baik. Sistem ini harus dapat mempermudah dan memperlancar proses pendaftaran registrasi peserta dan dapat meningkatkan keamanan sistem registrasi event. Hal ini sangat penting agar tidak terjadi kesalahan atau duplikasi data yang dapat menyebabkan kekacauan pada saat pelaksanaan kegiatan. Sistem registrasi yang dibuat harus dapat digunakan dengan efektif, efisien, dan aman saat digunakan, sehingga pada saat proses registrasi pendaftaran, registrasi ulang, dan pengelolaan data menjadi lebih cepat sehingga dapat menghilangkan antrian registrasi ulang peserta yang cukup panjang dan lama. Selain itu, sistem ini juga harus dapat mengamankan identitas peserta agar tidak disalahgunakan sehingga tercipta rasa nyaman dan aman pada peserta. Maka dari itu, penelitian ini akan menerapkan algoritma AES 256 pada QR code untuk sistem registrasi event sepeda gunung.

Volume 13 Number 2, July 2023 Page. 286-300
Journal Homepage: http://teknois.unbin.ac.id/index.php/JBS
DOI Link: http://doi.org/10.36350/jbs.v13i2

2. Permasalahan

a. Berdasarkan Teknologi yang digunakan saat ini belum efektif dan efisien dalam mengelola data peserta, sehingga saat proses registrasi ulang memakan waktu yang cukup lama.
b. Berdasarkan Teknologi yang digunakan saat ini registrasi event sangat rentan terjadinya kebocoran data mengingat 1 akun digunakan Bersama sama dengan panitia lain.

3. Tujuan

a. Menerapkan keamanan pada identitas peserta event sepeda gunung agar tidak terjadi kebocoran data.
b. Memudahkan dan mempercepat proses registrasi pendaftaran maupun registrasi ulang sehingga tidak membutuhkan waktu antrian yang lama.
c. Memudahkan admin registrasi dalam melakukan proses pengelohan data peserta

4. Tinjauan Pustaka

Kriptografi adalah sebuah Teknik untuk mengamankan sebuah pesan yang akan di trasmisikan melalui suatu jaringan dengan media elektronik tertentu kepada penerima agar keaslian isi pesan tersebut tidak berubah. Untuk menjalankan proses kriptografi terdapat beberapa tahapan yang saling berkaitan satu dengan yang lainya yaitu:

a. Plain Text adalah teks asli yang akan dienkripsi, biasanya berupa data atau pesan yang ingin diamankan.
b. Cipher Key adalah kunci yang digunakan untuk melakukan enkripsi dan dekripsi. Kunci ini harus disepakati sebelumnya antara pengirim dan penerima pesan agar pesan dapat dienkripsi dan didekripsi dengan benar.
c. Enkripsi adalah proses mengubah Plain Text menjadi Cipher Text menggunakan algoritma tertentu dengan bantuan Cipher Key. Enkripsi dilakukan untuk menjaga kerahasiaan pesan dari orang yang tidak berwenang.
d. Cipher Text adalah hasil dari enkripsi yang berupa teks terenkripsi atau data yang sudah diacak. Cipher Text tidak dapat dibaca oleh orang yang tidak memiliki kunci enkripsi yang tepat.
e. Dekripsi adalah proses mengembalikan Cipher Text menjadi Plain Text menggunakan kunci yang sama dengan yang digunakan pada saat enkripsi. Proses dekripsi dilakukan oleh penerima pesan untuk membaca pesan yang sudah dienkripsi oleh pengirim pesan.

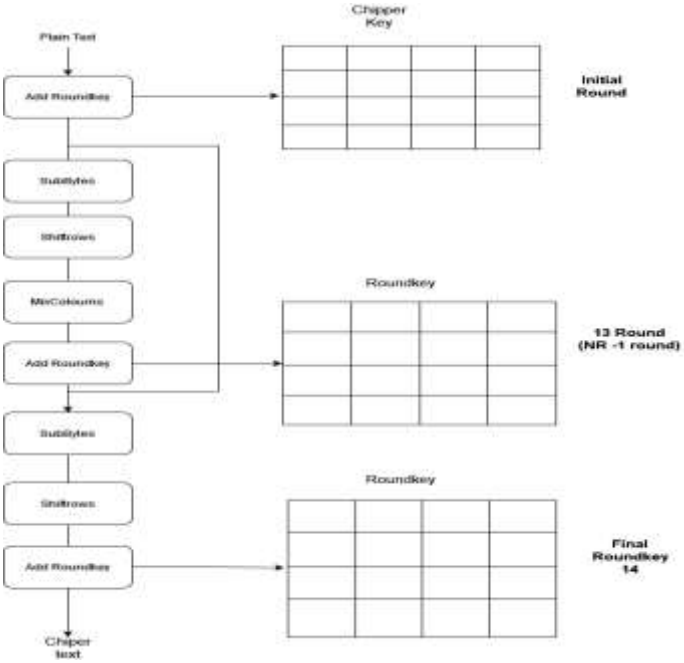
B. METODE

1. Metode Penelitian

Enkripsi pada algoritma AES 256 memiliki beberapa langkah yang harus di selesaikan berikut dapat dilihat pada gambar 1.

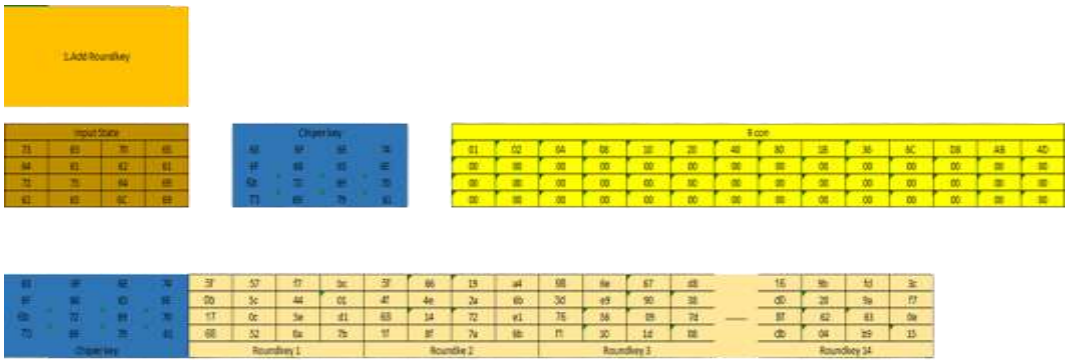
Enkripsi AES-256 dilakukan dengan menggunakan beberapa tahapan. Tahap awal adalah plaintext dan roundkey pertama. Pada tahap ini, plaintext yang akan dienkripsi dan roundkey awal yang digunakan akan di-XOR-kan satu sama lain. Hasil dari XOR ini kemudian akan menjadi input pertama untuk tahap berikutnya. Setelah itu, tahap kedua adalah substitusi dengan tabel s-box. Substitusi ini dilakukan dengan cara mengganti setiap byte input dengan byte yang sesuai dari tabel s-box. Tabel s-box adalah tabel pengganti yang digunakan untuk mengacak urutan bit pada byte input. Setelah hasil substitusi dengan s-box didapatkan, tahap berikutnya adalah shiftrows. Pada tahap shiftrows, urutan byte pada masing-masing baris di-shift ke kiri. Baris pertama tidak bergeser, baris kedua bergeser satu byte ke kiri, baris ketiga bergeser dua byte ke kiri, dan baris keempat bergeser tiga byte ke kiri. Setelah tahap shiftrows, tahap berikutnya adalah mixcolumns. Pada tahap mixcolumns, setiap kolom dari blok input akan dikalikan dengan sebuah matriks yang sudah ditentukan sebelumnya. Setelah tahap mixcolumns, maka didapatkan roundkey untuk putaran selanjutnya. Proses ini diulang kembali hingga putaran ke-13. Pada putaran ke-14, proses yang dilakukan untuk mendapatkan addroundkey adalah hanya melalui tahap substitusi dan shiftrows. Tidak ada lagi tahap mixcolumns yang dilakukan pada putaran ini. Setelah tahap terakhir ini selesai, maka didapatkanlah ciphertext sebagai hasil akhir dari proses enkripsi AES-256.

Volume 13 Number 2, July 2023 Page. 286-300
Journal Homepage: http://teknois.unbin.ac.id/index.php/JBS
DOI Link: http://doi.org/10.36350/jbs.v13i2



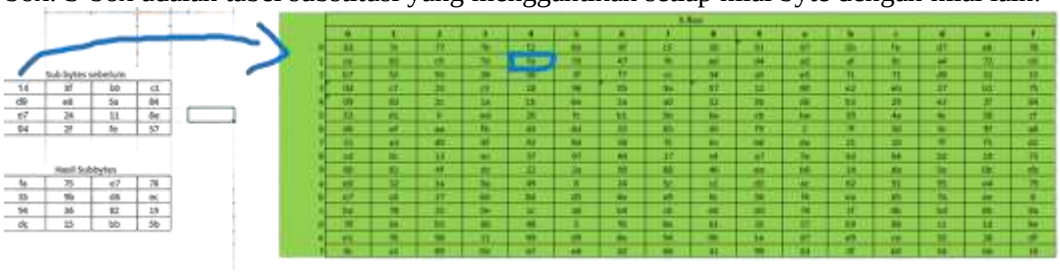
Gambar 1 Alur Algoritma AES

a. Gambar 2 Proses Enkripsi – input state dan chipper mendfinisikan Matriks input state akan di-"XOR"-kan dengan kunci enkripsi pertama (Round Key 0) untuk menghasilkan state awal.



Gambar 2 Proses Enkripsi-Add roundkey

b. Proses enkripsi – subbytes adalah tahap pertama dalam enkripsi AES-256 yang melibatkan penggantian setiap byte pada matriks ke input state dengan byte yang sesuai dari tabel S-box. S-box adalah tabel substitusi yang menggantikan setiap nilai byte dengan nilai lain.



Gambar 3 Proses Enkripsi-Subbytes

c. Proses enkripsi -Shiftrows adalah salah satu tahap pada proses enkripsi AES-256 yang dilakukan setelah proses SubBytes. Pada tahap ini, setiap baris state array akan digeser secara sirkular ke kiri. Baris pertama tidak digeser, baris kedua digeser sebanyak satu byte, baris ketiga digeser sebanyak dua byte, dan baris keempat digeser sebanyak tiga byte.

Volume 13 Number 2, July 2023 Page. 286-300
Journal Homepage: http://teknois.unbin.ac.id/index.php/JBS
DOI Link: http://doi.org/10.36350/jbs.v13i2

				Shiftrows
fa	75	e7	78	
35	9b	d6	ec	Bergeser 1 byte
94	36	82	19	bergeser 2 byte
dc	15	bb	5b	bergeser 3 byte

Gambar 4 Proses enkripsi – shiftrows

d. Proses enkripsi – MixColumns merupakan salah satu tahapan dalam enkripsi AES yang bertanggung jawab untuk mengubah setiap kolom pada matriks state (dalam bentuk byte) menjadi kolom baru yang berbeda. Proses ini melibatkan perkalian matriks kolom state dengan matriks konstan 4x4 tertentu

MixColumns sebelum

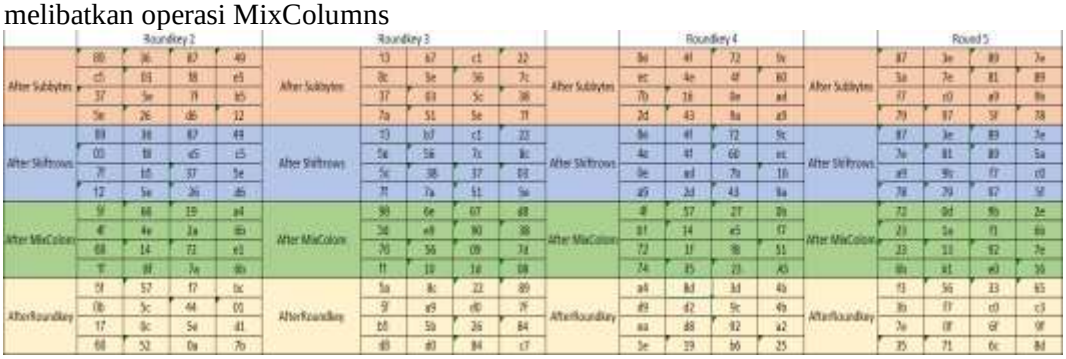
13	b7	c1	22
5e	56	7c	8c
5c	38	37	03
7f	7a	51	5e

Hasil MixColumns

19	3d	54	36
24	3f	85	6b
3d	26	6f	41
27	8c	57	b2

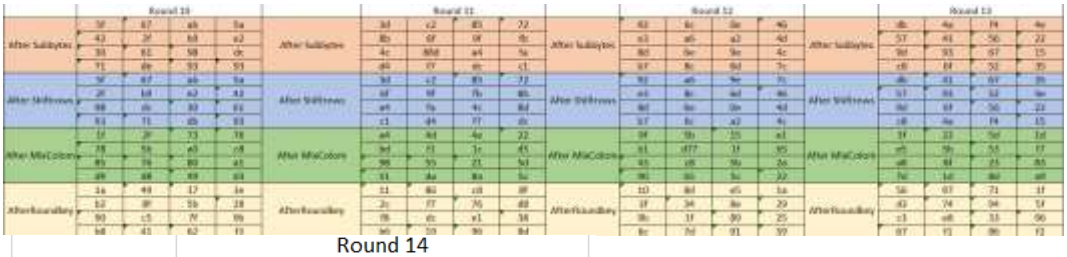
Gambar 5 Proses Enkripsi – MixColumns

e. Hasil Enkripsi AES 256 yang terdapat pada gambar 6 sampai gambar 7 Hasil enkripsi pada AES-256 adalah ciphertext yang terdiri dari 16 byte atau 128 bit dalam bentuk heksadesimal. Ciphertext tersebut dihasilkan dari proses enkripsi yang menggunakan plaintext dan chiper key sebagai input. Proses enkripsi AES-256 dilakukan dengan melakukan serangkaian putaran (round) dengan setiap putaran terdiri dari empat operasi dasar yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Putaran terakhir tidak melibatkan operasi MixColumns



Gambar 6 Hasil enkripsi Algoritma Aes 256

Volume 13 Number 2, July 2023 Page. 286-300
Journal Homepage: http://teknois.unbin.ac.id/index.php/JBS
DOI Link: http://doi.org/10.36350/jbs.v13i2

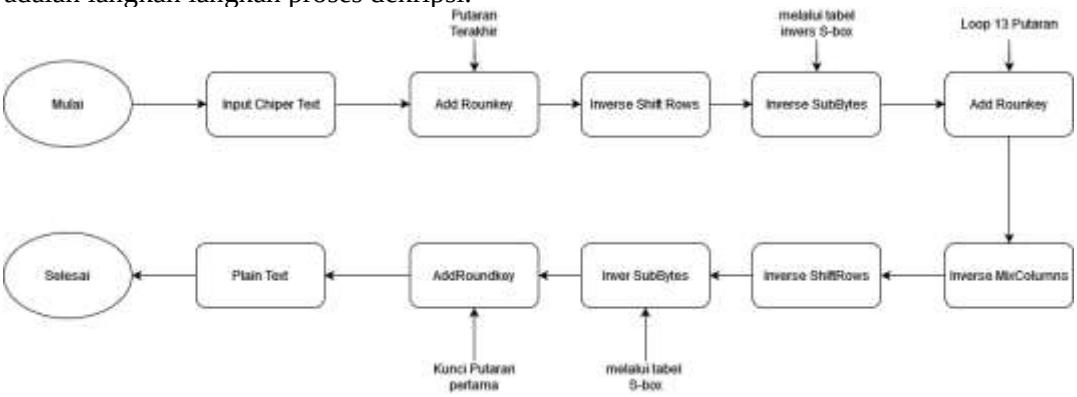


Round 14

After Subbytes	d4	89	55f	f7
	d5	1e	4c	e5
	c1	c4	cc	2f
	08	c9	9b	5a
After Shiftrows	d4	89	5f	f7
	1e	4c	e5	d5
	cc	2f	c1	c4
	5a	08	c9	6b
AfterRoundkey	16	9b	fd	3c
	d0	20	9a	f7
	8f	62	63	0e
	db	04	b9	15

Gambar 7 Hasil Algoritma AES 256 putaran 14

f. Proses Dekripsi pada gambar 8 Merupakan Langkah yang hampir mirip dengan proses enkripsi, namun urutan subkey (round key) yang digunakan dibalik urutannya berikut adalah langkah langkah proses dekripsi.



Gambar 8 Proses alur Dekripsi

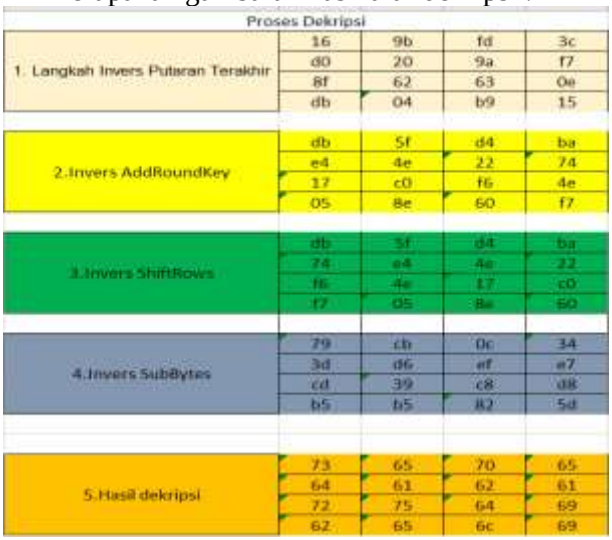
Berikut adalah penjelasan proses alur dekripsi:

a. Cipher Text dan Round Keys: Alur proses dimulai dengan input Cipher Text dan Round Keys (sama seperti pada proses enkripsi). Cipher Text adalah teks yang telah dienkripsi sedangkan Round Keys adalah kunci acak yang digunakan pada setiap putaran enkripsi.
b. AddRoundKey: Pada tahap ini, Cipher Text akan di XOR dengan round key yang telah dipilih dan dibentuk pada proses enkripsi. Proses ini dilakukan untuk mengembalikan nilai plaintext yang sesuai dengan kunci yang digunakan pada proses enkripsi.
c. Invers Shift Rows: Pada tahap ini, Cipher Text diubah kembali ke bentuk matriks 4x4 dan kemudian dilakukan invers shift rows. Proses invers shift rows adalah proses kebalikan dari shift rows pada proses enkripsi, di mana setiap baris pada matriks Cipher Text akan digeser ke kanan.
d. Invers SubBytes: Pada tahap ini, setiap elemen pada matriks Cipher Text akan diubah kembali ke plaintext melalui invers substitusi dengan S-box yang sama seperti pada proses enkripsi. Proses ini dilakukan untuk mengembalikan nilai plaintext dari nilai yang telah diubah pada proses enkripsi.
e. Invers MixColumns: Pada tahap ini, dilakukan invers mix columns untuk mengembalikan nilai plaintext asli. Proses invers mix columns dilakukan dengan menggunakan matriks invers yang berbeda dari matriks mix columns pada proses enkripsi.

Volume 13 Number 2, July 2023 Page. 286-300
Journal Homepage: http://teknois.unbin.ac.id/index.php/JBS
DOI Link: http://doi.org/10.36350/jbs.v13i2

f. Tahap 2-5: Tahap 2 hingga 5 akan dilakukan secara berulang hingga tahap 14, dimana pada tahap ini hanya dilakukan invers shift rows, invers subbytes, dan addroundkey.
g. Plaintext: Setelah tahap 2-5 selesai dilakukan sebanyak 14 putaran, maka nilai plaintext yang asli akan didapatkan sebagai output akhir dari alur proses dekripsi.

Pada Gambar di bawah ini merupakan gambaran hasil alur dekripsi :



Gambar 9 Proses Dekripsi

2. Teknik Analisis Data

Dalam penelitian ini, metode analisis data yang digunakan adalah dengan menggunakan presentase kelayakan. Kuesioner yang digunakan menggunakan skala Likert dengan lima pilihan jawaban. Rumus yang digunakan untuk menghitung presentase kelayakan adalah

$$Persentase\ kelayakan(\%) = \frac{Skor\ yang\ diobservasi}{Skor\ yang\ di\ harapkan} X100\%$$

Hasil presentase digunakan untuk memberikan jawaban atas tingkat kelayakan dari aspek-aspek yang diteliti. Pembagian kategori kelayakan terdiri dari lima kategori, yaitu sangat baik, baik, cukup, kurang, dan sangat kurang. Skala ini memperhatikan rentang dari bilangan presentase, dengan nilai maksimal yang diharapkan adalah 100% dan minimum 0%. Pembagian rentang kategori kelayakan dapat dilihat pada tabel yang disediakan:

Tabel 1. Kategori kelayakan

Presentase Pencapaian	Interpretasi
< 21%	Sangat Tidak Layak
21% - 40%	Tidak Layak
41% - 60%	Cukup layak
61% - 80%	Layak
81% - 100%	Sangat Layak

Untuk mengetahui kelayakan digunakan tabel diatas sebagai acuan penilaian data yang dihasilkan dari validasi pengguna dari skala likert

3. Instrumen Pengumpulan Data

Instrumen yang digunakan dalam penelitian ini adalah kuesioner. Terdapat 2 macam jenis pertanyaan yaitu pertanyaan tertutup dan pertanyaan terbuka. Pertanyaan tertutup berisi pertanyaan-pertanyaan untuk mengetahui kualitas produk dan fitur-fitur serta fungsionalitas sistem perangkat lunak secara keseluruhan, sementara jenis pertanyaan terbuka berisi saran atau kritik terkait dengan produk yang dikembangkan. Instrumen yang digunakan meliputi pengujian oleh ahli dan pengujian oleh pengguna:

a. Instrumen Untuk Ahli

Dalam pengujian oleh ahli, metode analisis black box digunakan dengan membuat sebuah instrument berupa pertanyaan yang digunakan untuk mengukur dan menilai hasil

keputusan. Sedangkan pada pengujian oleh pengguna, kuesioner diberikan kepada subjek uji coba untuk mengetahui kelayakan dan ketepatan informasi yang dihasilkan. Pertanyaan yang diajukan antara lain:

1. Apakah proses penanganan data registrasi peserta dengan adanya sistem basis data menjadi lebih mudah?
2. Apakah kinerja fungsionalitas sistem registrasi event sepeda menjadi lebih efisien?
3. Apakah tampilan sistem mudah dipahami dan digunakan?
4. Apakah proses registrasi ulang menjadi lebih cepat?
5. Apakah penerapan algoritma enkripsi AES dan QR Code efektif dalam mengamankan identitas peserta?

b. Instrument pengguna

Menurut(Sufandi and Aprijani, 2022) Pada kesimpulannya bahwa Dengan menggunakan PSSUQ yang terdiri dari 19 pertanyaan yang dibagikan kepada 140 orang dapat disimpulkan bahwa secara umum aplikasi dapat diterima dengan baik oleh pengguna, baik dari sisi kegunaan aplikasi (Sysuse), kualitas informasi (Infoqual), dan kualitas antarmuka (Interqual), serta kepuasan aplikasi secara keseluruhan untuk pengguna.Instrumen pengumpulan data dalam penelitian ini adalah kuesioner yang disebarkan kepada pengguna sistem registrasi event sepeda. Instrumen ini terdiri dari beberapa pertanyaan yang digunakan untuk mengukur kepuasan pengguna terhadap sistem yang dikembangkan. Kuesioner ini diolah menggunakan nilai rata-rata dan melakukan uji signifikansi untuk mengetahui signifikansi perbedaan tingkat kepuasan responden. Pengolah data pengujian data dibagi menjadi beberapa bagian kuesioner, yaitu Overall, System Usefulness, Information Quality, dan Interface Quality. Kuesioner ini digunakan untuk menilai kinerja sistem registrasi event sepeda dan mengetahui kekurangan yang ada dalam sistem untuk dapat diperbaiki:

Tabel 2. Kuesioner pengguna

No	Pernyataan	Responden				
		1	**2**	**3**	**4**	**5**
1	Tampilan sistem registrasi event sepeda ini menimbulkan rasa aman dalam menyimpan informasi pribadi saya					
2	Tampilan registrasi jelas dan mudah dipahami					
3	Proses pengisian registrasi sangat mudah dan cepat					
4	Sistem registrasi sangat mudah dipahami dan digunakan					
5	Sistem registrasi ulang dengan QR code sangat mudah dipahami dan digunakan					
6	Sistem registrasi ulang dengan QR code lebih efektif					
7	Sistem registrasi ulang dengan QR code lebih efisien					
8	Mekanisme registrasi ulang sederhana dan mudah digunakan					
9	Sistem registrasi ini cukup lengkap untuk memenuhi kebutuhan data peserta					
10	Pilihan opsi daftar event sangat membantu untuk memilih event yang diinginkan					
11	Pilihan opsi kategori memudahkan dalam menemukan kategori kelas yang diinginkan.					

12	Sistem ini telah menjamin keamanan data peserta					
13	Sistem registrasi event sepeda ini membuat saya percaya dalam melakukan proses registrasi					
14	Sistem registrasi event sepeda ini dapat meningkatkan efisiensi proses antrian pada saat registrasi ulang					
15	Sistem registrasi ini jauh lebih baik dibandingkan menggunakan google form					
16	Sistem registrasi ini meningkatkan keamanan dalam memberikan informasi seputar identitas pribadi					
17	Sistem registrasi ini lebih efektif dibandingkan sistem registrasi sebelumnya					
18	Sistem registrasi ini lebih aman dibandingkan sistem sebelumnya					
19	Sistem registrasi ini lebih unggul dari segi efektivitas, efisiensi dan keamanan dibandingkan sistem sebelumnya.					

Terdapat empat tanggapan PSSUQ, dan tanggapan itu adalah Overall, Overall adalah Skor kepuasan secara keseluruhan, jadi total nilai keseluruhan adalah Overall, lalu ada Sysuse, Sysuse adalah kegunaan sistem atau teknologi, seberapa berguna atau bermanfaatkah sistem dan teknologi pada penelitian ini, dan terdapat juga Infoqual, Infoqual adalah tingkat kualitas data yang diperoleh, dan terakhir adalah Interqual, Interqual adalah tingkat kualitas interface/antarmuka, karena interface aplikasi sangat penting, hal yang pertama dilihat pengguna adalah interface atau antarmuka aplikasi. Dan berikut tabel standar penilaian skor PSSUQ :

Tabel 3. Aturan PSSUQ

Nama Skor	Skor (rata – rata Item Respon)
OVERALL	Pertanyaan no 1 s/d 19
SYSUSE	Pertanyaan no 12-19
INFOQUAL	Pertanyaan no 3,-11
INTERQUAL	Pertanyaan no 1-2

Untuk mengevaluasi lebih dalam lagi, berikut ada beberapa pertanyaan terbuka yang akan diajukan kepada responden untuk mendapatkan masukan yang konstruktif terkait dengan produk yang akan dibuat. Tabel berikut ini menampilkan 5 pertanyaan terbuka yang akan diajukan kepada pengguna:

Skala Likert digunakan untuk mengukur sikap, pendapat, dan persepsi terhadap fenomena sosial. Dan hasil dari setiap pertanyaan kuesioner yang menggunakan skala lekert memiliki nilai sangat positif sampai sangat negatif, dan dalam kuesioner penelitian ini, terdapat 5 jenis jawaban didalam setiap pertanyaan. Berikut adalah penilaian yang dilakukan dengan sistem skor, dan setiap pertanyaan diberi skor berikut ini :

Tabel 4. Penilaian skala likert

No	Kategori	Nilai
1	Sangat Setuju	5
2	Setuju	4
3	Netral	3
4	Tidak Setuju	2
5	Sangat Tidak Setuju	1

Volume 13 Number 2, July 2023 Page. 286-300
Journal Homepage: http://teknois.unbin.ac.id/index.php/JBS
DOI Link: http://doi.org/10.36350/jbs.v13i2

C. HASIL DAN PEMBAHASAN

1. HASIL

a. Hasil Analisa Kebutuhan

Metode algoritma AES dan QR code diperlukan untuk meningkatkan efisiensi dan keamanan dalam proses registrasi sepeda yang belum optimal. Tahap-tahap yang akan dilakukan meliputi:

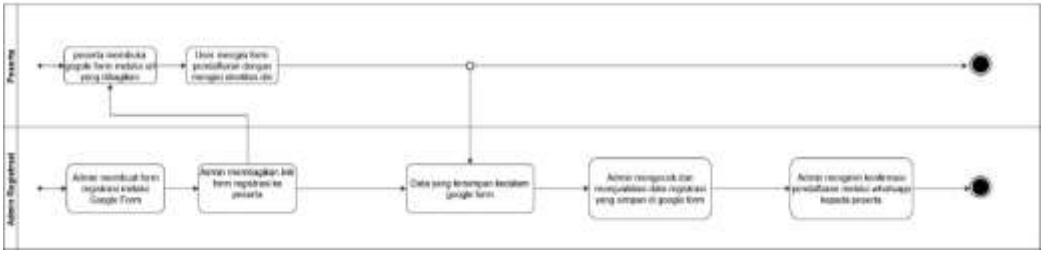
1) Proses pengumpulan dokumen

Pengembang melakukan analisis terhadap data yang ada. Dari hasil analisis tersebut, ditemukan bahwa data tersebut masih berantakan dan tidak terstruktur, sehingga menyulitkan panitia dalam proses pengolahan data.

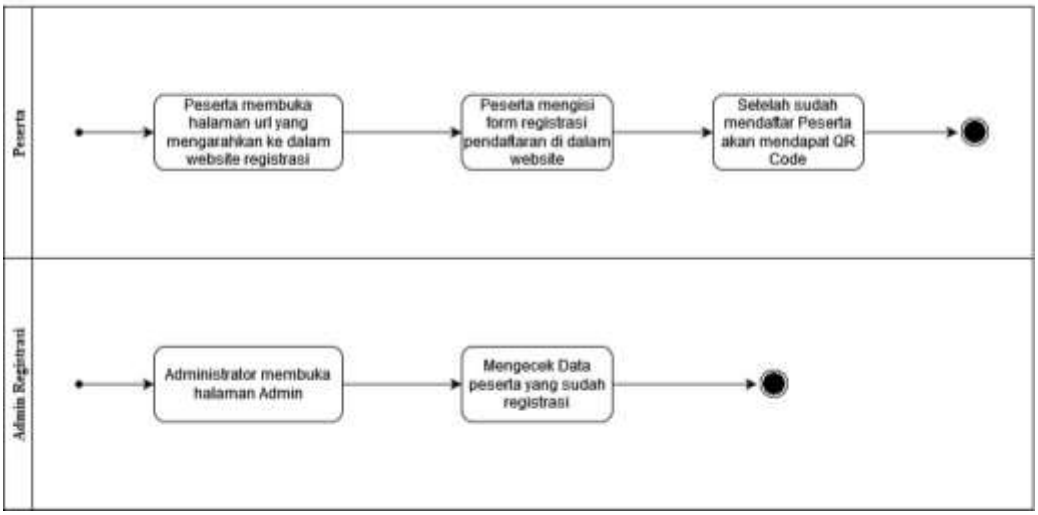
2) Pembuatan proses bisnis baru yang menggunakan metode algoritma AES dan QR code.

Proses bisnis yang digunakan sebelumnya cukup efektif dalam memudahkan peserta dalam melakukan pendaftaran, namun dari sisi panitia, proses tersebut kurang efektif karena kesulitan dalam mengolah data yang diperoleh. Oleh karena itu, akan dikembangkan proses bisnis baru yang menggunakan metode algoritma AES dan QR code untuk meningkatkan efisiensi dan keamanan dalam proses registrasi event sepeda

Pada proses registrasi lama, peserta harus menunggu selesainya proses validasi dari administrator. Kemudian, setelah diperiksa dan lulus dari validasi administrator, konfirmasi pendaftaran dikirimkan kepada peserta melalui WhatsApp,Sedangkan pada proses registrasi baru Nampak jelas perbedaanya jauh lebih efektif dan efisien,peserta hanya perlu melakukan registrasi melalui website, mengisi data diri setelah data diyakinkan sesuai peserta akan mendapat QR Code yang berisi data peserta yang telah di enkripsi dan akan QR Code tersebut digunakan pada saat nanti registrasi ulang, Administrator hanya perlu masuk ke halaman admin untuk mengecek data peserta yang telah melakukan registrasi



Gambar 10. Proses bisnis registrasi lama

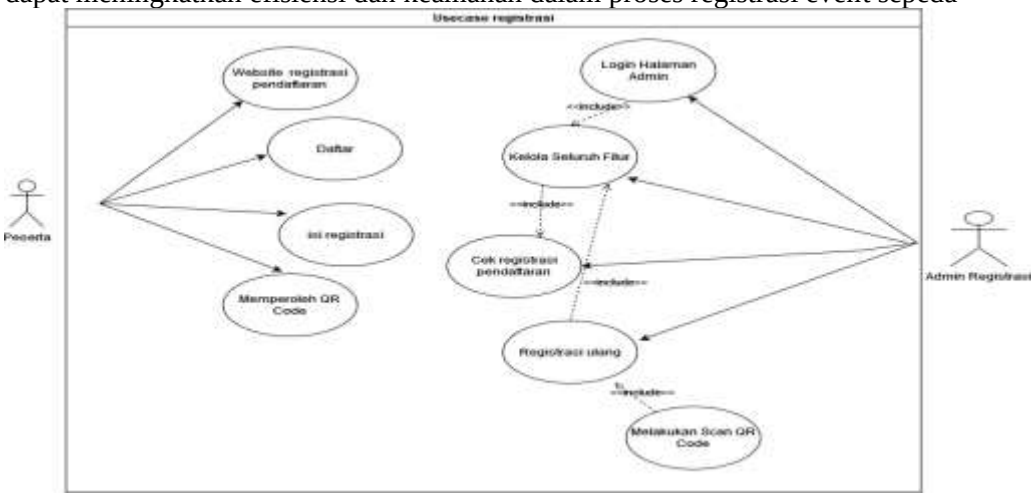


Gambar 11. Proses registrasi baru

Pemrosesan data peserta dilakukan dengan menggunakan Algoritma AES dan QR code. Setelah data peserta diinput, peserta akan menerima QR code yang berisi data

Volume 13 Number 2, July 2023 Page. 286-300
Journal Homepage: http://teknois.unbin.ac.id/index.php/JBS
DOI Link: http://doi.org/10.36350/jbs.v13i2

peserta yang telah dienkripsi. Administrator dapat melakukan verifikasi data peserta yang terdaftar dengan mengscan QR code yang diterima peserta. Hal ini diharapkan dapat meningkatkan efisiensi dan keamanan dalam proses registrasi event sepeda



Gambar 12. Usecase diagram

Pada Gambar diatas, dijelaskan bahwa terdapat dua aktor dalam proses registrasi event sepeda. Aktor pertama adalah peserta, yang melakukan input data registrasi melalui website yang disediakan. Setelah melakukan pendaftaran, peserta menerima QR code yang berisi data yang telah dienkripsi, yang akan digunakan pada saat registrasi ulang. Aktor kedua adalah admin yang bertugas mengelola data registrasi pendaftaran, melakukan verifikasi dengan men-scan QR code yang diterima peserta, dan mengelola fitur-fitur yang ada di halaman admin.

b. Pengkodean Algoritma AES 256

Gambar 13. Fungsi Controller

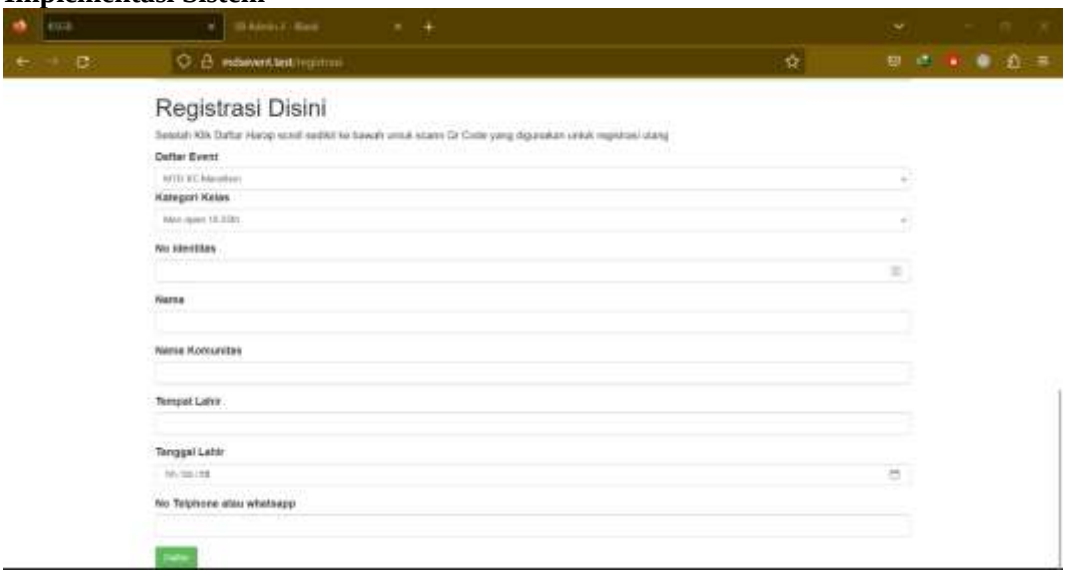
Pada gambar diatas, dijelaskan langkah awal untuk mengenkripsi sebuah data, dengan metode AES 256 maka kita memerlukan panjang key sebanyak 32 karakter yang akan digunakan untuk mengenkripsi.

Volume 13 Number 2, July 2023 Page. 286-300
Journal Homepage: http://teknois.unbin.ac.id/index.php/JBS
DOI Link: http://doi.org/10.36350/jbs.v13i2

Gambar 14. Fungsi Deskripsi

Fungsi Dekripsi adalah script untuk men-dekripsi isi pesan yang di-enkrip, jika key sesuai maka pesan dapat di-dekripsi.

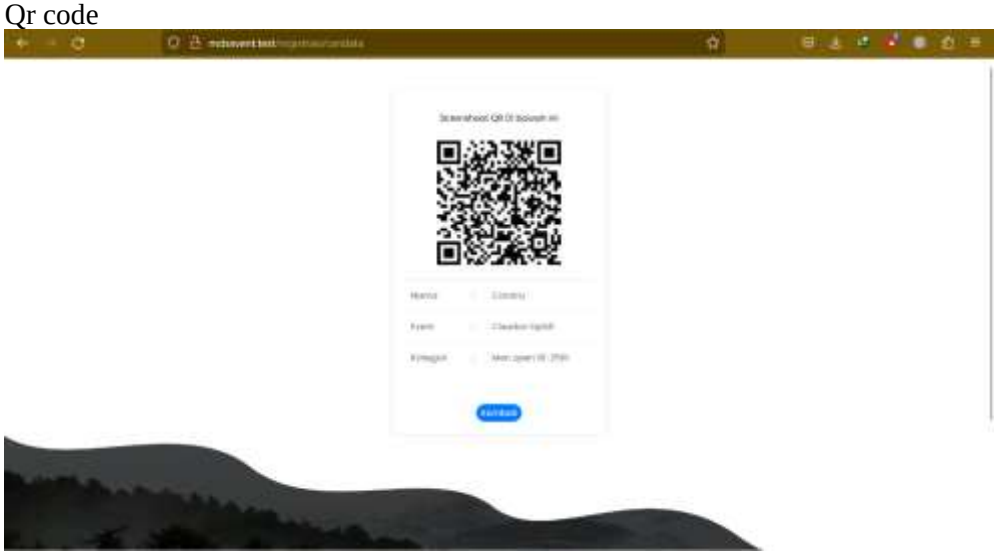
c. Implementasi Sistem



Gambar 15. Halaman Registrasi peserta

Pada gambar diatas merupakan halaman registrasi peserta, peserta hanya perlu klik link yang di dapat dari panitia yang membagikan link registrasi. peserta hanya perlu mengisi data diri tidak perlu login.

1.) Qr code



Gambar 17. Peserta mendapatkan QR code

Volume 13 Number 2, July 2023 Page. 286-300
Journal Homepage: http://teknois.unbin.ac.id/index.php/JBS
DOI Link: http://doi.org/10.36350/jbs.v13i2

Pada Gambar 15 merupakan proses setelah melakukan pendaftaran peserta akan mendapat Qr Code yang digunakan untuk registrasi ulang.

2.) Hasil Qr code yang sudah di enkripsi

Gambar 16. Hasil Qr Code yang terenkripsi

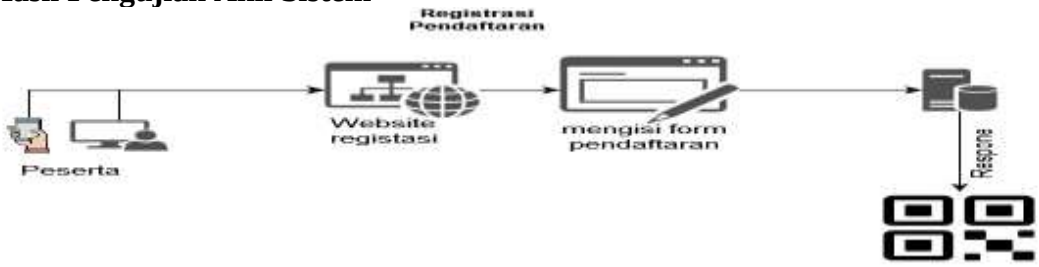
3.) Tampilan Qr Code di buka melalui pengguna

Gambar 17. Hasil QR tidak terbaca diluar system

Pada gambar diatas, dijelaskan jika melakukan scan QR melalui smartphone dan di buka pada browser tidak akan dapat bisa terbaca, dikarena QR tersebut hanya dapat dibaca oleh sistem yang meng generatenya.

2. PEMBAHASAN

a. Hasil Pengujian Ahli Sistem



Gambar 18 Proses registrasi pendaftaran

Pada gambar 18 Merupakan Proses Registrasi peserta, dapat dilihat bahwa peserta hanya perlu melakukan input data pada halaman website registrasi yang telah disediakan. Kemudian, setelah mendaftar, peserta akan menerima QR code yang berisi data peserta yang telah dienkripsi menggunakan Algoritma AES.kemudian Qr tersebut digunakan untuk registrasi ulang agar mendapatkan racepack dan no BIB.

Gambar 19. Proses Registrasi ulang

Volume 13 Number 2, July 2023 Page. 286-300
Journal Homepage: http://teknois.unbin.ac.id/index.php/JBS
DOI Link: http://doi.org/10.36350/jbs.v13i2

Pada Gambar 19 Peserta Hanya perlu datang ke meja panitia dan menunjukan Qr code yang didapatkan dari hasil pendaftaran peserta, kemudian Panitia Registrasi akan melakukan scan dengan alat scanner barcode kepada QR code peserta, secara otomatis akan membaca isi QR tersebut akan terbaca oleh sistem kemudia peserta akan mendapatkan racepack dan no bib.

b. Tahap Uji coba produk

Tahap uji produk dilakukan untuk mencari tahu karakteristik data untuk setiap masing masing variabel. Hasil dari kelayakan yang telah diuji melalui hasil kuesioner menentukan hasil yang diharapkan. Berikut dapat ditampilkan pada tabel hasil perhitungan kelayakan tersebut

Tabel 5 Hasil uji coba produk

Responden H	Jenis tanggapan PSSUQ			
	Overall	Sysuse	Infoqual	Interqual
asil R1	82	34	40	8
R2	77	32	37	8
R3	88	37	41	10
data R4	83	33	40	10
R5	90	39	41	10
Total skor	420	175	199	46
Total maksimal skor	500	200	250	50
Presentase kelayakan	84	70	79,6	92

hitungan kelayakan didapatkan presentase kelayakan sebesar 84% Maka berdasarkan skala likert apabila presentase mencapai 84% - 100% bisa dikategorikan sebagai “sangat layak”. Kuesioner yang telah diberikan beserta dengan pertanyaan pendukung yang mencakup kritik dan saran untuk dari responden, Kritik dan juga saran yang telah diberikan akan menjadi bahan evaluasi untuk sistem yang sedang dikembangkan

D. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan, kesimpulan yang dapat diuraikan antara lain:

1. Menerapakan algoritma aes 256 pada qr code dapat meningkatkan keamanan identitas peserta yang bersifat pribadi sehinga data tidak mudah untuk di untuk di bocorkan.
2. Penerapan algoritma AES 256 pada QR code dapat meningkatkan efektivitas dan efisiensi proses registrasi pendaftaran peserta maupun registrasi ulang peserta event sepeda gunung.
3. Dengan adanya sistem registrasi ini yang lebih mudah dan cepat, proses pengelolaan data peserta dapat dilakukan secara efisien oleh admin.

E. DAFTAR PUSTAKA

[1]. Martawireja, A. R. (2021). Proteksi Keamanan Data pada Quick Response (QR) Code. Jurnal Teknologi dan Rekayasa Manufaktur, 99-110.
[2]. Nurnaningsih, D. (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes). Jurnal Teknik Informatika, 177-186.
[3]. Nurnaningsih and Permana, 2018. Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes). Retrieved from https://journal.uinjkt.ac.id/index.php/ti/article/view/7811/pdf

[4]. Paramarta, Kusyanti and Data, 2018. Implementasi Algoritme Advance Encryption Standard (AES) pada Enkripsi dan Dekripsi QR-Code.Retrieved From https://ojs.unsiq.ac.id/index.php/jebe/article/view/2151
[5]. Pariddudin, A., & Syauqi, F. (2020). Penerapan Algoritma AES pada QR CODE untuk Keamanan Verifikasi Tiket. *TeknoIS : Jurnal Ilmiah Teknologi Informasi dan Sains*, *10*(2), 43-52. doi:https://doi.org/10.36350/jbs.v10i2.87
[6]. Rosa A.S, M. (2015). Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek. bandung: informatika bandung.
[7]. Sufandi, U. U. (2022). Pengukuran Usability Aplikasi Web Menggunakan Metode Pssuq (Study Kasus: Aplikasi Sitta Universitas Terbuka). JST (Jurnal Sains dan Teknologi), 249-256.
[8]. Sufandi and Aprijani, 2022. Pengukuran Usability Aplikasi Web Menggunakan Metode Pssuq (Study Kasus: Aplikasi Sitta Universitas Terbuka) https://ejournal.undiksha.ac.id/index.php/JST/article/view/43534