Implementasi Sistem Deteksi Katarak Berbasis Website Menggunakan Algoritma *Advanced Encryption Standard* (AES) Dan Algoritma Rivest Code 4 (RC4)

Implementation Of A Website-Based Cataract Detection System Using The Advanced Encryption Standard (AES) Algorithm And Rivest Code 4 (RC4) Algorithm

1st Shalsabila Azzahra
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
shalsabilazzhr@student.telkomuniversity.ac.id

2nd Sussi
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
sussiss@telkomuniversity.ac.id

3rd Bagus Aditya
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
goesaditya@telkomuniversity.ac.id

Abstrak—Katarak merupakan penyakit pada mata yang merupakan penyebab nomor satu kebutaan, oleh karena itu penanganan katarak harus dianggap serius dengan melakukan kontrol rutin ke dokter mata.Namun mengunjungi rumah sakit secara berkala tidak efisien untuk masyarakat khususnya masyarakat yang sibuk bekerja dan berada jauh di pedesaan. Sistem deteksi katarak untuk diagnosa dini dibutuhkan agar masyarakat dapat dengan mudah melakukan pengecekan matanya secara rutin. Maka dari itu, Tugas Akhir berpusat pada desain dan implementasi sistem deteksi katarak berbasis *website* menggunakan algoritma *Advanced Encryption Standard* (AES) dan Algoritma *Rivest Code* (RC4). Sistem ini dirancang untuk membantu pengguna dalam mendeteksi matanya secara dini dengan mengeluarkan diagnosa mata normal, matur, dan immatur. Desain sistem pada *website* yang dirancang adalah pengguna melakukan *scanning* pada matanya lalu data berupa *image* akan dikirim ke API *Server* Heroku lalu data akan diklasifikasikan dan dikirim ke firebase untuk di enkripsi selanjutnya data akan dikirim kembali ke website untuk di dekripsi dan diagnosa pun akan muncul. Dilakukan dua pengujian terhadap algoritma AES-256 dan RC4 dari sisi *performance* dan durasi enkripsi, Dari pengujian kedua algoritma tersebut didapat hasil bahwa AES-256 memiliki nilai rata-rata *Avalanche Effect* antara 45% - 60% sedangkan RC4 memiliki nilai rata-rata *Avalanche Effec*t di atas 70%, sedangkan untuk waktu durasi enkripsinya AES-256 memiliki rata-rata waktu sebesar 90.3 s sedangkan RC4 sebesar 18 s. Berdasarkan hasil pengujian *Quality of Service* dari pengiriman data FCS *website* hingga ke API *Server* (Heroku) menghasilkan nilai rata-rata *throughput* sebesar 747.22 Kbps, *packet loss* sebesar 0.12% dan *delay* sebesar 24.1 s.

Kata kunci — katarak, *web application*, *advanced Encryption Standard* (AES), *Rivest Code* 4 (RC4).

Abstract—Cataract is a disease of the eye which is the number one cause of blindness, therefore cataract management must be taken seriously by conducting regular check-ups with an ophthalmologist. A cataract detection system for early diagnosis is needed so that people can

easily check their eyes regularly. Therefore, this final project focuses on the design and implementation of a website-based cataract detection system using the Advanced Encryption Standard (AES) and Rivest Code (RC4) algorithms. This system is designed to assist users in detecting their eyes early by issuing normal, mature, and immature eye diagnoses. The system design on the website that is designed is that the user scans his eyes and then the data in the form of an image will be sent to the Heroku API Server then the data will be classified and sent to firebase for encryption, then the data will be sent back to the website for decryption and a diagnosis will appear. Two tests were carried out on the AES-256 and RC4 algorithms in terms of performance and duration of encryption. above 70%, while for the duration of encryption AES-256 has an average time of 90.3 s while RC4 is 18 s. Based on the Quality of Service test results from sending FCS website data to the API Server (Heroku) the average throughput value is 747.22 Kbps, packet loss is 0.12% and delay is 24.1 s.

Keywords: cataract, web application, advanced Encryption Standard (AES), Rivest Code 4 (RC4).

I. PENDAHULUAN

Katarak merupakan suatu penyakit pada mata yang pengidapnya memiliki lensa mata yang berawan dan keruh. Secara umum, katarak dapat dibedakan menjadi dua kelas sesuai dengan tingkat toleransinya, yaitu katarak imatur dimana katarak ini adalah jenis yang masih bisa ditoleransi artinya penyembuhannya tidak perlu melewati operasi. Dan katarak matur merupakan katarak yang tidak bisa ditoleransi artinya penyembuhannya harus melalui operasi. Pencegahan katarak dapat dilakukan dengan cara pemeriksaan mata secara rutin ke rumah sakit setiap tahunnya agar dapat mendeteksi katarak sejak dini[1]. Namun hal ini dirasa tidak efisien untuk masyarakat yang tinggal dipedesaan maupun yang sibuk bekerja. Oleh karena itu, dibutuhkan suatu sistem kecerdasan buatan atau dapat disebut juga kecerdasan algoritma untuk membantu masyarakat mendeteksi katarak secara rutin tanpa harus pergi ke dokter. Melalui penelitian sebelumnya dikembangkanlah desain dan implementasi sistem deteksi katarak menggunakan algoritma Convolutional Neural Network (CNN) berbasis *website*. Penggunaan aplikasi website dipilih karena memiliki kelebihan daripada aplikasi mobile yang diantaranya tidak semua masyarakat bersedia untuk meng-*install* aplikasi pada *smartphone*, *website* dapat di akses oleh masyarakat yang tidak memiliki *handphone* yang memadai dan dapat menghemat *storage*, serta jika dilihat dari *website developer* kelebihannya yaitu lebih menghemat biaya pasalnya aplikasi website lebih mudah dibuat, dilakukan *update* serta *maintenance*. Pada klasifikasi ini, hasilnya dibagi menjadi tiga kelas yaitu matur, imatur, dan normal. Serta penggunaan website sebagai platform untuk mendeteksi keberadaan katarak agar lebih mempermudah masyarakat karena diakses langsung tanpa harus memeriksakan lagi ke dokter spesialis mata. Masyarakat hanya perlu melakukan registrasi dengan memasukkan data pribadi pada website, selanjutnya melakukan *scanning* mata pada *webcam* hasil vonis pun akan muncul sesuai dengan kondisi masing-masing mata.

Dalam suatu *website* yang berhubungan dengan data pribadi seseorang, diperlukan suatu sistem keamanan, pasalnya beberapa waktu silam terjadi kasus kebocoran data milik pasien Covid-19, data yang berkapasitas 720 GB atau terdiri dari 6 juta data pasien ini dijual di forum online Raid. Sementara itu, perlindungan hukum tentang kerahasiaan data kesehatan pasien juga diatur dalam undang-undang nomor 36 tahun 2009 karena data kesehatan merupakan aspek yang sangat penting dan privasi[2]. Oleh karena itu, penulis mengimplementasikan algoritma enkripsi *Advanced Encryption Standard* (AES) dan *Rivest Code* 4 (RC4) sebagai algoritma kriptografi yang melindungi data pada *website* untuk selanjutnya dilihat keakurasiannya dan di implementasikan pada *website*. Harapannya dengan pembuatan aplikasi website ini, pengguna dapat memeriksakan keadaan matanya secara rutin dan dini dengan keamanan data yang terjamin.

II. METODE

A. Tinjauan Pustaka

1. Katarak

Katarak merupakan suatu penyakit dimana lensa mata mengalami kekeruhan sehingga penglihatan menjadi buram. Lensa mata terletak dibelakang pupil yang berfungsi untuk memperjelas cahaya yang masuk lewat pupil agar masuk tepat ke retina sehingga objek dapat terlihat dengan jelas. Lensa terbentuk oleh protein dan air, semakin bertambahnya usia jumlah protein semakin menumpuk lalu menggumpal sehingga mulai membentuk area kecil seperti kabut pada lensa hal inilah yang disebut katarak. Katarak dapat terjadi bukan hanya

pada lansia tetapi disemua umur tidak terkecuali bayi[3].

2. Convolutional Neural Network (CNN)

Algoritma CNN adalah sejenis metode jaringan syaraf tiruan yang memiliki akurasi tinggi dalam pengklasifikasiannya. Terdapat tiga layer utama dalam proses pengerjaan klasifikasi gambar menggunakan algoritma CNN yaitu *Convolutional Layer, Pooling Layer*, dan *Full Connected Layer*. Convolutional Layer digunakan untuk mengekstrak fitur data yang akan digunakan untuk training, kemudian lapisan penyatuan digunakan untuk membuat filter baru berdasarkan aturan yang dibuat, dan akhirnya terhubung sepenuhnya menjadi lapisan sebenarnya yaitu MLP (*Multilayer Perceptron*)[4].

3. Website

Website adalah kumpulan beberapa informasi berupa teks, gambar, ilustrasi dan video yang saling tergabung pada sebuah domain atau URL dalam bentuk halaman. Halaman-halaman ini hanya bisa diakses oleh koneksi internet. Halaman web dibentuk oleh format HTML *(Hyper Text Markup Language)* dan di akses melalui HTTP. HTTP meneruskan informasi dari server agar muncul pada tampilan web yang berbentuk statis ataupun dinamis yang saling terkait membentuk rangkaian dan dihubungkan dengan *hyperlink*[5].

4. Firebase

Firebase adalah software suatu *Database Realtime* yang berfungsi untuk koordinasi otomatis aplikasi milik client yang terhubung firebase jadi jika ada pembaharuan dari aplikasi client maka data yang ada pada firebase berubah pula. Firebase terdapat pada *cloud* serta *support multiplatform* seperti Web, Android dan iOS. Data pada firebase berbentuk JSON (*Java Script Object Natation*). Beberapa fitur yang terdapat pada firebase yaitu: *Analytics*, *Develop*, dan *Grow*[6].

5. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) atau sering dikenal dengan algoritma Rijndael adalah algoritma kriptografi untuk pengamanan data. Algoritma AES memiliki kunci kriptografi 128,192, dan 256 bits namun memiliki ukuran kunci blok asli 128 bit. Dalam proses pengiriman datanya terdapat *plaintext* dan *cipher text*. Pesan awal yang belum dienkripsi dinamakan *plaintext* dan pesan yang sudah dienkripsi dinamakan *cipher text*[7].

6. Cipher Block Chaining

CBC bertujuan membuat blok-blok saling ketergantungan, memakai vector inisialisasi yang berukuran tertentu sesuai dengan ukuran satu blok plaintext. Alur kerja CBC yaitu plaintext dipisah menjadi beberapa bagian blok, selanjutnya plaintext akan di XOR dengan IV fungsinya agar pola dari plaintext tersembunyi. Lalu blok-blok tersebut akan dienkripsi sampai menghasilkan ciphertext, prosesnya berurut dari mulai blok plaintext pertama. Ciphertext yang sudah dienkripsi digunakan sebagai IV untuk proses selanjutnya yaitu penyandian blok plaintext. Berikut merupakan skema enkripsi *Cipher Block Chaining*[8].

7. Base64

Transformasi Base64 adalah algoritma yang menggunakan enkripsi modern berasal dari pengkodean transfer MIME yang merupakan sekelompok skema pengkodean biner ke teks serupa yang mewakii data biner sebagai teks ASCII yang perlu disimpan dan di transfer lalu menerjemahkannya kedalam representasi radix-64. Hal ini bertujuan untuk memastikan data tetap utuh tanpa termodifikasi selama proses transportasi. Algoritma Base64 memiliki tiga bit yang masing-masing terdiri dari delapan bit dan mengubahnya masing-masing menjadi empat bit[9].

8. RC4

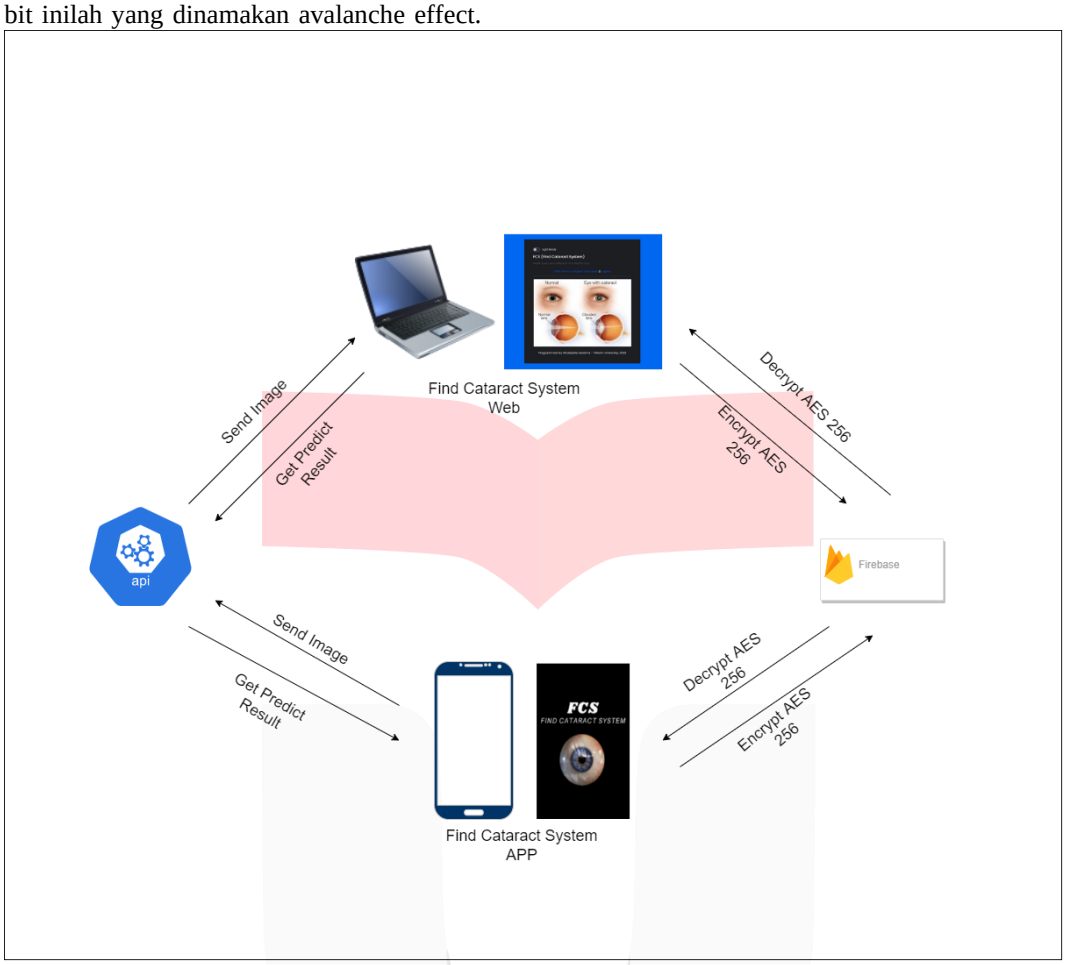
RC4 (Rivest Code 4) adalah sebuah algoritma kriptografi yang memakai kunci yang jenisnya sama untuk mengenkripsi dan mendeskripsikan sebuah data, pesan, maupun informasi maka RC4 termasuk ke dalam algoritma kriptografi simetris. RC4 terbagi menjadi dua bagian yaitu penghasilan kunci enkripsi dan inisialisasi state-array. RC4 memiliki panjang kunci dari 1 sampai 256 bit yang dipakai untuk menginisialisasikan tabel sepanjang 256 bit. Lalu state-array yang tersedia akan di acak lalu diproses untuk mendapatkan kunci enkripsi yang kemudian dilakukan XOR menghasilkan *plaintext* ataupun *cyphertext*[10].

9. Avalanche Effect

Avalanche effect merupakan karakteristik penting untuk algoritma enkripsi. Ini menjadi acuan apakah suatu

algoritma enkripsi memiliki kualitas atau nilai yang baik atau tidak. Ini dapat dilihat ketika mengubah satu bit atau lebih dalam plaintext lalu menghasilkan bit berubah untuk putaran berikutnya. Hasil perubahan bit inilah yang dinamakan avalanche effect. Nilai avalanche effect dikatakan baik apalagi bernilai 40% hingga 60%[11].

B. Desain Sistem

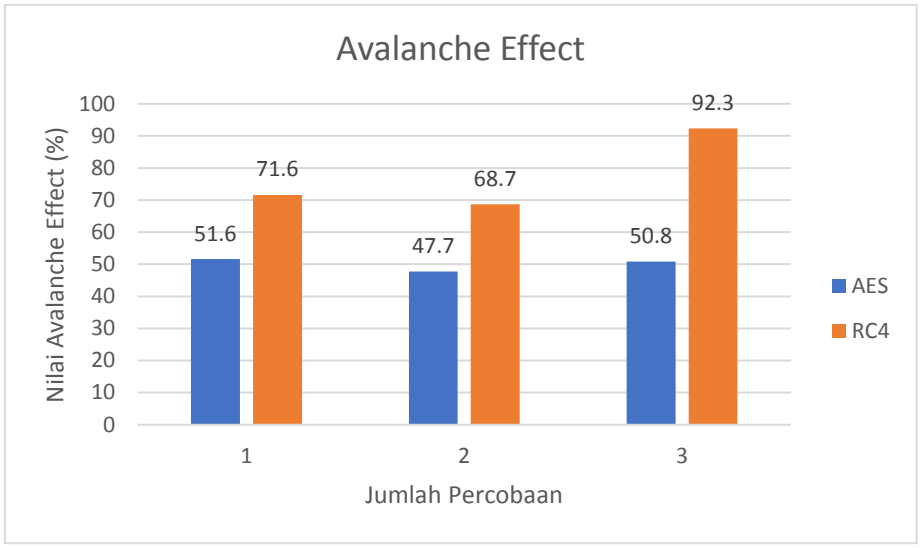


GAMBAR 1
DESAIN SISTEM

Gambar 1. menjelaskan proses kerja sistem web, user diharuskan melakukan registrasi untuk membuat akun lalu melakukan login. Masuk ke *dashboard* web, lalu melakukan *inspect* mata pada *webcam*. Gambar yang terdeteksi lalu dikirim ke API *Server* (Heroku) menggunakan base64 (pengubahan dari gambar ke binary lalu text). Pada Heroku data diubah menjadi bentuk gambar menggunakan base64 dan di klasifikasikan berdasarkan data normal, matur, atau imatur lalu diubah lagi menjadi teks. Selanjutnya hasil prediksi dikirim ke firebase untuk disimpan dan di enkripsi, selanjutnya hasil diagnosa di dekripsi pada FCS web lalu tampilah hasilnya.

III. HASIL DAN PEMBAHASAN

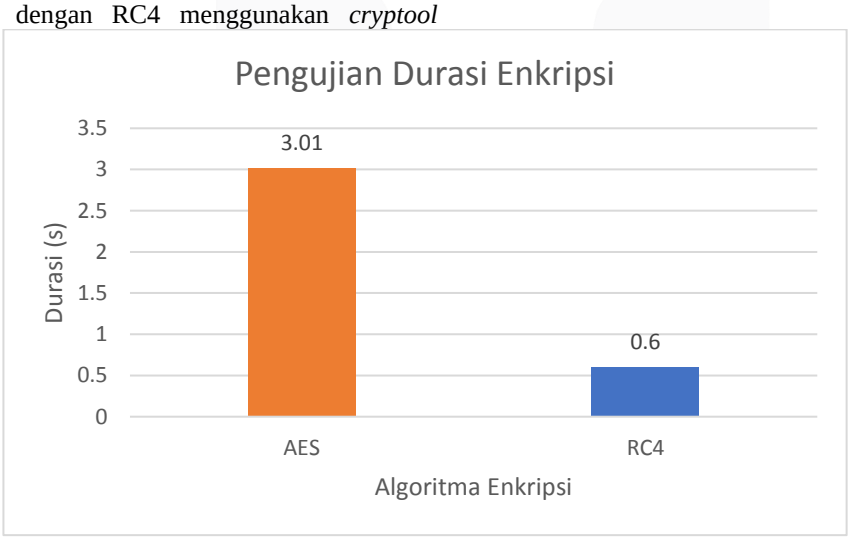
A. Hasil Analisis Tingkat Keamanan AES dan RC4 berdasarkan *Avalanche Effect*



GAMBAR 2
PENGUJIAN AVALANCHE EFFECT AES DAN RC4

. Pada pengujian AES didapatkan hasil yang cukup baik dikarenakan menghasilkan nilai yang ideal yaitu diatas 45% namun dibawah 60%. dilakukan pula tiga kali percobaan untuk avalanche effect RC4 didapatkan nilai diatas 60% artinya nilai tidak terlalu baik karena hasil tersebut diatas dari nilai ideal. Pengujian avalanche effect AES-256 dengan RC4 menggunakan *cryptool* berbeda, jika AES-256 dilakukan pengubahannya pada plaintext yang sudah di ubah menjadi biner, sedangkan pada RC4 percobaan pengubahannya pada plaintextnya langsung.

B. Hasil Pengujian Kecepatan Durasi Enkripsi



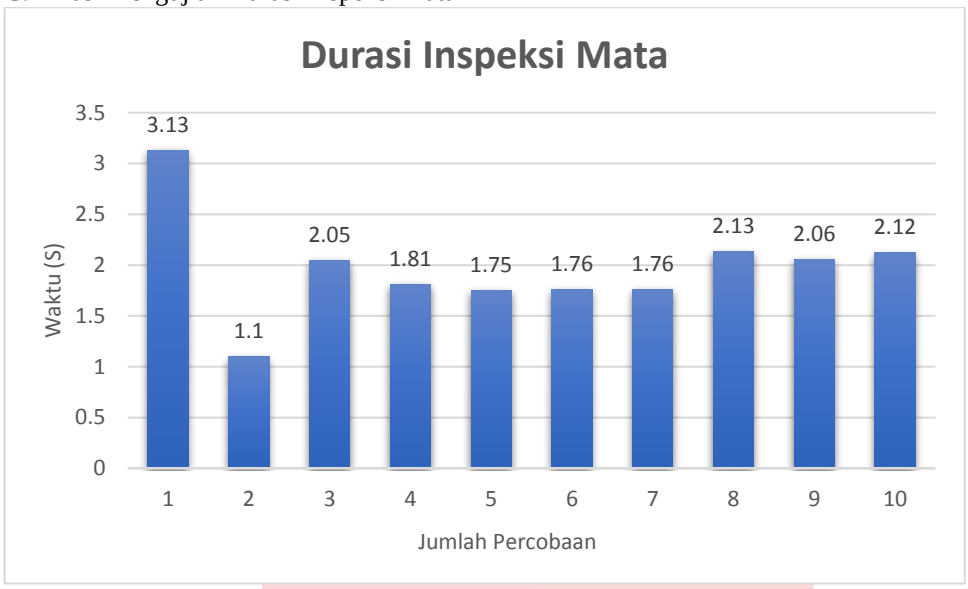
GAMBAR 3
GRAFIK PENGUJIAN DURASI ENKRIPSI

Dilakukan sebanyak tiga puluh kali pengujian menggunakan tipe password *weak* hingga *strong* dan dihasilkan total sebesar 90.3 s untuk AES 256 bit dan 18 s untuk RC4 serta rata rata nya adalah 3.01 s untuk AES 256 dan 0.6 s untuk RC4. Berdasarkan **Gambar 3** dihasilkan nilai rata-rata yang cukup jauh antara enkripsi AES 256 bit dengan RC4 hal ini dikarenakan secara arsitektur AES 256 bit mempunyai 14 round hal ini lebih kompleks dibandingkan dengan arsitektur enkripsi RC4. Sehingga durasi waktu yang dibutuhkan AES 256 bit lebih lama.

Berdasarkan dua pengujian diatas, penulis memutuskan untuk memakai AES 256 bit untuk FCS website. Hal ini dikarenakan penulis menggunakan algoritma enkripsi yang tingkat keamanannya lebih tinggi yaitu AES 256 bit sesuai dengan yang

sudah dibuktikan pada pengujian avalanche effect.

C. Hasil Pengujian Durasi Inspeksi Mata

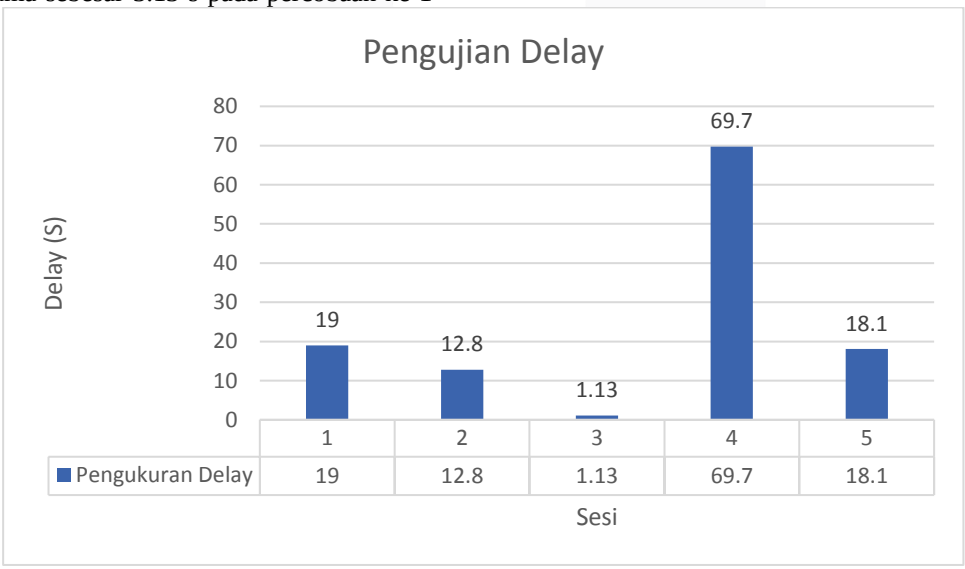


GAMBAR 4
DURASI INSPEKSI MATA

Dilakukan pengujian terhadap durasi yang dibutuhkan untuk melakukan inspeksi mata pada FCS website mulai dari user melakukan scanning mata hingga hasilnya keluar, skenario pengujian dengan menggunakan 10 kali tes mata yang dilakukan dengan webcam. Terdapat waktu terlama sebesar 3.13 s pada percobaan ke 1 dan waktu tercepat pada percobaan ke 2 yaitu 1.1 s. Nilai rata-rata durasi inspeksi mata adalah sebesar 1.9 s.

D. Hasil Pengujian Performansi Jaringan dengan Quality of Service

1. Hasil Pengujian Delay

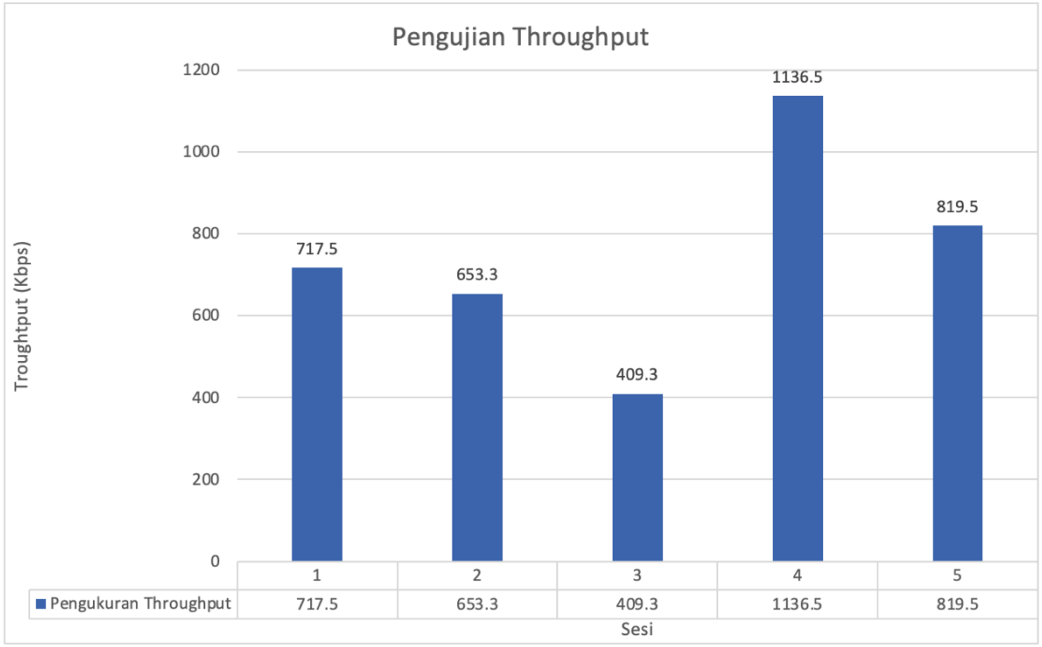


GAMBAR 5
GRAFIK PENGUJIAN DELAY

Pengujian delay dilakukan dengan menggunakan software wireshark dengan memfilter paket data TCP. Di dapat nilai rata-rata dari pengujian delay adalah sebesar 24.1 s dengan delay terbesar terdapat pada sesi 4 yaitu sebesar 69.7 s dan delay terkecil terdapat pada sesi 3 yaitu sebesar 1.13 s. Terdapat lonjakan delay pada sesi 4 dikarenakan data yang masuk besar pada sesi tersebut sehingga performa network menurun. Namun untuk nilai rata-rata delay saat pengujian dikatakan masih cukup aman

karena masih memenuhi standar nilai ITU-TG.1010 yaitu *Preferred* < 15 s, *Acceptable* < 60 s.

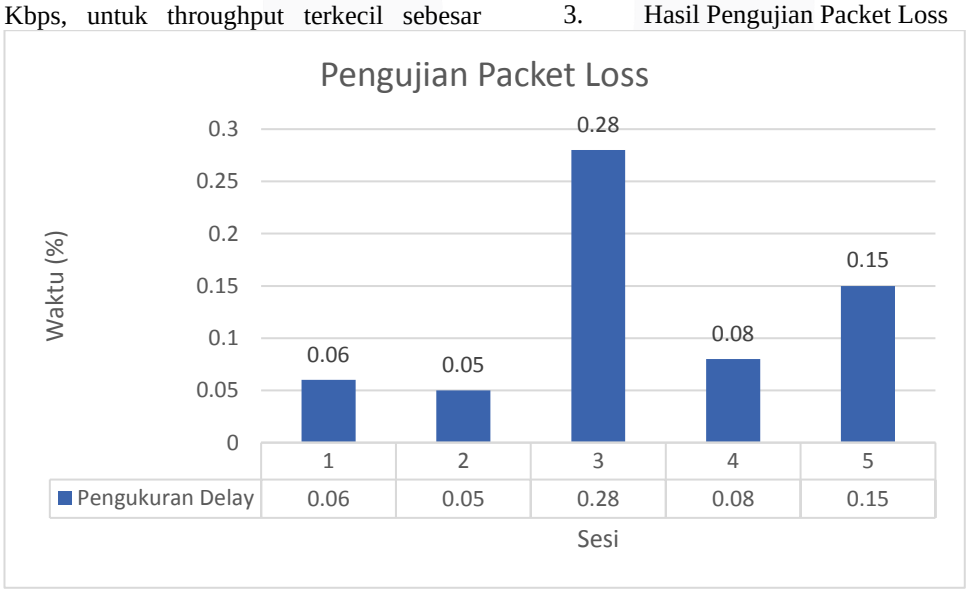
2. Hasil Pengujian Throughput



GAMBAR 6
GRAFIK PENGUJIAN THROUGHPUT

Pengujian throughput dilakukan dengan menggunakan software Wireshark dengan memfilter paket data TCP dengan IP server Heroku. Pengujian memakai internet wifi mncplay 15mbps. Didapat rata-rata hasil pengujian throughput yaitu sebesar 747.22 Kbps, untuk throughput terkecil sebesar 409.3kb/s terdapat pada sesi 3 dan throughput terbesar adalah 1136.5kb/s pada sesi 4. Rata-rata hasil pengujian per sesinya cukup signifikan karena keadaan koneksi internet serta spesifikasi server dan perangkat.

3. Hasil Pengujian Packet Loss



GAMBAR 7
GRAFIK PACKET LOSS

Pengujian packet loss dilakukan dengan menggunakan software wireshark dengan memfilter paket data TCP menggunakan tcp.analysis.ack_lost_segment dan IP server Heroku di dapat hasil rata-rata dari pengujian packet loss yaitu 0.12, untuk packet loss terkecil terdapat pada sesi 2 yaitu sebesar 0.05 dan untuk packet loss terbesar terdapat pada sesi 3 sebesar 0.28. Berdasarkan nilai

standar pada ITU-TG.1010 nilai packet loss seharusnya 0 atau tidak ada packet loss tetapi ditemukan packet loss dengan nilai yang cukup kecil pada pengujian ini dikarenakan saat pengujian ada sedikit gangguan sinyal.

IV. KESIMPULAN

1. Sistem deteksi katarak berbasis website menggunakan algoritma *advanced encryption standard* (AES) dan algoritma *rivest code* 4 (RC4) secara keseluruhan berjalan dengan baik sehingga *users* sudah dapat menggunakan website ini untuk mengetahui vonis awal dari kondisi matanya.
2. Menggunakan algoritma AES-256 dan RC4 untuk pengamanan FCS Website yang proses enkripsinya diletakkan pada bagian registrasi data diri dan hasil inspect mata di firebase dan dekripsi terdapat pada hasil diagnosa di website.
3. Berdasarkan dua pengujian yang dilakukan untuk melihat tingkat keamanan diantara algoritma AES-256 dan RC4, penulis menggunakan pengujian Avalanche Effect dan mendapatkan nilai rata-rata AES-256 sebesar 50.3% sedangkan RC4 sebesar 77.6%. Menurut standar, nilai Avalanche Effect yang baik adalah antara 45-60% sehingga dapat diambil kesimpulan bahwa AES-256 memiliki tingkat keamanan yang lebih tinggi dibanding RC4, hal ini selaras dengan pengujian durasi enkripsi AES-256 memerlukan waktu yang lebih lama ketimbang RC4 yaitu sebesar 90.3 s untuk 30 kali pengujian data sedangkan RC4 hanya memerlukan waktu 18 s untuk 30 kali pengujian proses enkripsi. Sehingga penulis memakai algoritma AES-256 untuk keamanan FCS Website.
4. Berdasarkan pengujian durasi inspeksi mata yang dilakukan saat scanning mata hingga hasilnya keluar didapatkan rata-rata yaitu 1.9 s.
5. Berdasarkan pengujian Quality of service di dapat nilai rata-rata throughput adalah sebesar 747.22 Kbps. Lalu untuk nilai rata-rata packet loss di dapat sebesar 0.12%. Selanjutnya untuk performansi delay, nilai rata-rata yang di dapat adalah sebesar 24.1 s dan termasuk angka yang masih aman menurut standar.

A. Saran

1. Menambahkan fitur *eye detection* pada *webcam* agar lebih mudah mendeteksi objek.
2. Menambahkan fitur *forget password* pada menu login agar memudahkan *users* jika lupa *password*.
3. Perlu dilakukan percobaan pengujian QoS dibeberapa waktu yang berbeda baik dalam kondisi jaringan internet yang sibuk maupun yang normal sehingga hasilnya lebih maksimal.

REFERENSI

[1] A. T. Sulistiyani, "Efektifitas Senam Mata," pp. 1-18, 2013.

[2] I. A. V. R. Y. Ade Utia Detty, "Karakteristik Faktor Risiko Penderita Katarak," *JIKSH: Jurnal Ilmiah Kesehatan Sandi Husada*, vol. 10, no. e-ISSN: 2654-4563 dan p-ISSN: 2354-6093, pp. 1-6, 2021.

[3] M. N. A. N. A. H. A. Dr. Yusra Haddeh, "eview of Cataract Types and Its Pathogenesis in Patients Reviewing Al Moujtahd Hospital in Damascus, Syria," *Journal of Medical Pharmaceutical and Allied Sciences* , vol. 7, no. 6, 756, pp. 1-7, 2018.

[4] A. J. N. C. A. P. A. Novia Farhan Nissa, "Application of Deep Learning Using Convolutional Neural Network (CNN) Method for Women's Skin Classification," *Scientific Journal of Informatics*, vol. 8, pp. 1-10, 2021.

[5] R. Harminingtyas, "ANALISIS LAYANAN WEBSITE SEBAGAI MEDIA PROMOSI, MEDIA TRANSAKSI DAN MEDIA INFORMASI DAN PENGARUHNYA TERHADAP BRAND IMAGE PERUSAHAAN PADA HOTEL CIPUTRA DI KOTA SEMARANG," *STIE SEMARANG*, vol. 6, no. 3, pp. 1-21, 2014.

[6] I. F. Maulana, "Penerapan Firebase Realtime Database pada Aplikasi E-Tilang Smartphone berbasisMobile Android," *Jurnal Resti*, vol. 4, no. 5, pp. 854-863, 2019.

[7] G. P. Rahul Lanjewar, "Implementation of AES-256 Bit: A Review," *Academia*, no. 3, pp. 1-6, 2015.

[8] P. R. Dinantaka, "Aplikasi Metode Enkripsi Cipher Block dan Stream Cipher Menggunakan Collision Resistant Hash

Function Untuk Pengamanan File Rahasia," vol. 2, no. 2, pp. 1-70, 2020.
[9] S. Gurpreet Singh, "Modified Vigenere Encryption Algorithm and its Hybrid Implementation with Base64 and AES," pp. 1-6, 2013.
[10] Z. Panjaitan, "Algoritma RC4 (Contoh Perhitungan Lengkap)," 20 Januari 2020. [Online]. Available: https://komputerkata.com/algoritma-rc4-contoh-perhitungan-lengkap/. [Accessed 2021].
[11] N. T. Amish Kumar, "Effective Implementation and Avalanche Effect of AES," vol. 1, pp. 1-5, 2012.