Perancangan Sistem Deteksi Katarak Berbasis Android Menggunakan Algoritma *Advanced Encryption Standard* (AES) Dan *Data Encryption Standard* (DES)

Android-Based Cataract Detection System Design Using Advanced Encryption Standard (AES) And Data Encryption Standard (DES) Algorithm

1st Atikah Nadilah
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
atikahnadilah@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—Menjadi rahasia umum bahwa katarak merupakan faktor utama penyebab kebutaan di dunia. Orang yang mengidap katarak merasa pandangannya menjadi keruh dikarenakan terdapat penumpukkan protein pada lensa mata. Oleh karena itu penyakit katarak mebutuhkan penanganan yang serius, biasanya seorang pasien yang mengidap katarak diperintahkan untuk melakukan *check up* rutin. Maka dirancanglah aplikasi android "FCS (*Find Cataract system)".* Pada Tugas Akhir ini, sebuah sistem deteksi katarak berbasis android dirancang untuk semua orang dari segala usia agar dapat dengan mudah melakukan *check up* secara berkala. Aplikasi android ini dirancang dengan menggunakan metode CNN (*Convolutional Neural Network*) dalam proses klasifikasinya. Selain iu, aplikasi ini dipastikan aman karena penulis meng-implementasikan model enkripsi terbaik dari enkripsi AES 256 dan DES. Hasil pengujian tingkat keamanan yang

terbaik menurut Avalanche effect untuk aplikasi *Find Cataract System* adalah AES 25 dengan rata-rata Avalanche effect 51.5% yang dimana masuk kedalam katagori terbaik untuk Avalanche effect. Adapun hasil pengujian *Quality of Service* dari aplikasi *Find Cataract System* didapat dengan rata-rata *delay* sebesar 7.17s, *throughput* sebesar 316,4 kbps dan *packet loss* sebesar 0%. Dan masuk kedalam QOS yang baik menurut ITU-T.

Kata kunci — katarak, advanced encryption standard, data encryption standard, android.

Abstract—It is common knowledge that cataracts are the main cause of blindness in the world. People who understand cataracts feel that their vision becomes cloudy because there is a buildup of protein in the lens of the eye. Because cataracts require serious treatment, a patient who has cataracts is usually ordered to have regular check-ups. Then the android application "FCS (Find Cataract system)" was designed.In this final project, an android-based cataract detection system is designed for people of all ages to easily perform regular check-ups. This android application is designed using the CNN (Convolutional Neural Network) method in the classification process. In addition, this application is ensured to be safe because the author implements the best encryption model of AES and DES encryption.The best security level

test results according to Avalanche effect for the Find Cataract System application is AES 25 with an average Avalanche effect of 51.5% which is in the best category for Avalanche effect. The results of the Quality of Service test from the Find Cataract System application were obtained with an average delay of 7.17s, throughput of 316.4 kbps and packet loss of 0%. And enter into good QOS according to ITU-T.

Keywords— cataract, advanced encryption standard, data encryption standard, android.

1. PENDAHULUAN

Katarak menjadi salah satu penyebab terbanyak kebutaan di dunia. Berdasarkan data dari *World Health Organization (WHO)* dari 39 juta kasus kebutaan di dunia sekitar 51% penduduk dunia mengalami kebutaan akibat katarak [1]. WHO memperkirakan sekitar hampir 20 juta penduduk populasi dunia menderita kebutaan akibat katarak, Indonesia sendiri merupakan salah satu negara dengan kasus kebutaan tertinggi karena katarak di dunia dengan jumlah penderita sekitar 0,78% dari jumlah populasi. Menurut survei *Rapid Assesment of Avoidable Blindness (*RABB) dari 15 provisi yang tersebar di Indonesia pada tahun 2013-2016 sekitar 70,8% persen diantara tingkat kebutaan di sebabkan oleh katarak [2].

Berdasarkan data masalah kasus kebutaan meningkat dari tahun ke tahun sehingga kita harus lebih peduli dengan Kesehatan mata dengan melakukan pemeriksaan dini. Diperkirakan insiden kasus penyakit katarak (penderita baru) sekitar 0.1% dari jumlah populasi, sehingga diperkirakan jumlah penderita baru katarak diiindonesia sekitar 250.000 orang per tahun (Kemenkes RI,2014) [3]. Hal ini tidak sebanding dengan jumlah dokter spesialis mata yang terbatas yaitu sekitar 3.000 orang dari seluruh Indonesia, bahkan juga tidak sebanding dengan kesenjangan fasilitas Kesehatan yang tersebar di Indonesia seperti di pedesaan [4].

Pada penelitian sebelumnya yang dibuat oleh Juyel Rana dan Syed Md. Galib yang membahas tentang deteksi katarak menggunakan *smartphone*, menjelaskan bahwa Dengan kurangnya dokter mata dan kamera slit lamp di daerah pedesaan, terutama dinegara berkembang seperti Bangladesh adalah masalah utama mendiagnosis katarak.Makalah ini menyajikan bukti-konsep aplikasi seluler pendeteksi katarak self-screening. Ini memungkinkan masyarakat untuk melakukan deteksi dini dengan menggunakan smartphone dengan kamera depan yang fokus dengan baik yang memungkinkan penyaringan mandiri dilakukan oleh hampir semua orang, kapan saja, di mana saja [5].

II. METODE

A. Tinjauan Pustaka

1. Katarak

Penyakit katarak merupakan proses degenerasi manula dimana terdapat kekeruhan pada lensa mata yang mempengaruhi penglihatan seseorang kabur, silau, memudar bahkan kebutaan. Kekeruhan ini terjadi akibat agregasi protein atau kerusakan serat pada kontak lensa [7]. Pada umumnya, penyakit katarak ini terjadi pada lansia namun saat ini ditemukan juga katarak di usia muda yaitu 30-40 tahun, hal ini disebabkan juga oleh kurangnya jumlah pemenuhan gizi dan nutrisi sesuai kebutuhan [8] .

2. Convolutional Neural Network (CNN)

Convolutional Neural Network (CNN) merupakan sebuah algoritma Deep Learning yang mampu mengolah data dua dimensi yang sampai saat ini menjadi metode klasifikasi yang memberikan hasil yang sangat baik. Maka pada penelitian kali ini metode CNN ini digunakan dalam machine learning untuk mengklasifikasi citra objek pada mata yang mengidap katarak [10].

3. Android

Android merupakan sebuah sistem operasi (*OS*) yang biasanya digunakan pada perangkat mobile seperti HP dan tablet. awalnya android merupakan sistem operasi seluler yang berbasiskan linux, Namun seiring berjalannya waktu perkembangan *android* semakin pesat menjadi sebuah *platform* yang begitu cepat dalam inovasinya. Hal ini tidak luput dari dukungan *Google* yang pertama kali mengakui *android* lalu membuatkan sebuah platform yang sampai saat ini bisa kita nikmati dengan leluasa [11].

4. Wireshark

Wireshark merupakan sebuah *tools* yang digunakan untuk menganalisis paket data dalam jaringan [14]. Wireshark sebelumnya juga dikenal dengan nama *Ethereal* juga dapat diartikan sebagai sebuah aplikasi yang dapat merekam atau meng-*capture* paket data berbasis *open-source* yang dapat digunakan untuk mengawasi serta menangkap trafik data dalam jaringan internet [15].

5. Firebase Cloud Messaging

Firebase cloud messaging (FCM) merupakan *web service* penyedia layanan

push notification atau pesan notifikasi serta juga sebagai jembatan antar server dengan perangkat *android* agar dapat terjadi *push notification* atau pengiriman pesan. FCM juga merupakan solusi pertukaran pesan lintas platform yang dapat Anda andalkan untuk mengirim pesan tanpa biaya [18].

6. Advanced Encryption Standard (AES)

Advanced Encryption Standard atau biasa disebut (AES) ini merupakan sebuah algoritma *cryptographic* yang dapat digunakan untuk mengamankan data. AES sendiri merupakan blok *chipertext* simetrix yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi sendiri merupakan proses penyandian *plaintext* menjadi *ciphertext*, atau pengubahan data menjadi bentuk rahasia. Dalam enkripsi AES ada 4 jenis proses transformasi bytes, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey* [21].

7. Data Encryption Standard (DES)

Data Encryption Standard merupakan sebuat algoritma enkripsi dengan jumlah penggunaan terbanyak di dunia. DES mengenkripsi data plaintext (data asli) dalam blok-blok 64 bit menjadi 64 bit data chipertext (data tersembunyi) dengan 56 bit kunci (*key*) [22]..

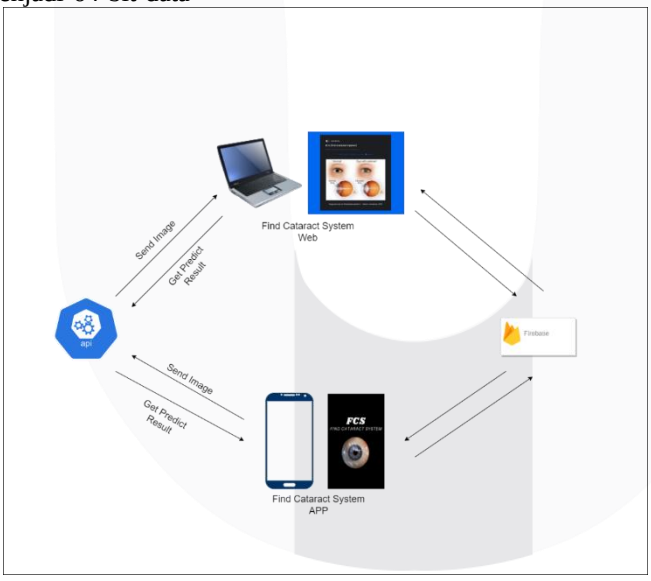
8. Parameter QOS

QOS atau *Quality of Service* merupakan parameter yang memiliki kemampuan untuk menyediakan layanan jaringan yang baik serta menyediakan *bandwith*, serta juga mengatasi permasalahan *jitter* dan *delay*. Kualitas jaringan sangat menentukan kualitas QOS, untuk membantu *Client* menjadi lebih bergunaserta memastikan user mendapatkan performansi yang lebih handal dari aplikasi jaringan lainnya. Parameter QOS merupakan kumpulan dari beberapa besaran teknis yaitu, *Throughput*, *Delay*, dan *Packet Loss* [23].

9. Avalanche Effect

Salah satu karakteristik untuk menentukan baik atau tidaknya suatu algoritma kriptografi adalah dengan melihat avalanche effect-nya. Suatu avalanche effect dikatakan baik jika perubahan bit yang dihasilkan berkisar antara 45-60% (50 % adalah hasil yang sangat baik) [24].

B. Desain Sistem

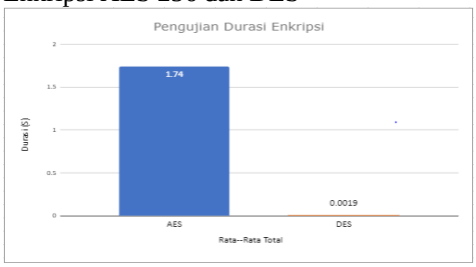


GAMBAR 1.
DESAIN SISTEM

Konsep dari *Find Cataract System* (FCS) dirancang untuk memudahkan user untuk memprediksi dini keadaan katarak pada mata agar efisien dan membantu memudahkan user untuk mengetahui Kesehatan mata, yang hasilnya dapat di diagnosa dalam 3 jenis keparahan yaitu mata normal, katarak imatur, serta katarak matur. Dari desain sistem diatas diketahui alur pemrosesan dari FCS bahwa data yang sudah diolah oleh *Machine Learning* akan dikirimkan ke *API server* untuk di dikirimkan ke *firebase* dan ditampilkan di halaman user.

III. HASIL DAN PEMBAHASAN

A. Hasil Pengujian Running Time Proses Enkripsi AES 256 dan DES

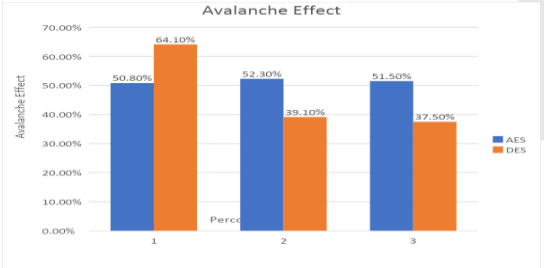


GAMBAR 2.
PENGUJIAN RUNNING TIME AES DAN DES

Dalam pengujian *running Time* pada aplikasi *android* ini menggunakan fungsi *System.currentTimeMillis*, untuk menguji hasil durasi enkripsi *AES* 256 dan *DES* pada aplikasi *find cataract system.* Pada grafik pertama menunjukan *running time* saat melakukan enkripsi *AES*, dapat dilihat bahwa *AES* memiliki rata-rata waktu pengujian 1,74s dengan waktu tercepat sekitar 1,62s dan waktu terlama sekitar 2,14s sedangkan pada grafik kedua menunjukan *running time* pengujian pada saat enkripsi *DES* memiliki rata-rata yaitu 0,0019 ms dengan waktu tercepat yaitu 0,001 ms dan waktu terlama sekitar 0,003 ms. Dari grafik ini diketahui bahwa dari segi kecepatan waktu enkripsi data enkripsi *DES* lebih cepat untuk mengenkripsi data dibandingkan dengan enkripsi *AES.* Pengujian ini dilakukan dengan menggunakan 30 sampel *password* dari *weak* dengan 6-8 karakter sampai *strong* dengan 18-20 karakter *password*.

B. Hasil Pengujian Tingkat Keamanan AES 256 dan DES

1. Perbandingan Avalanche Effect AES 256 dan DES

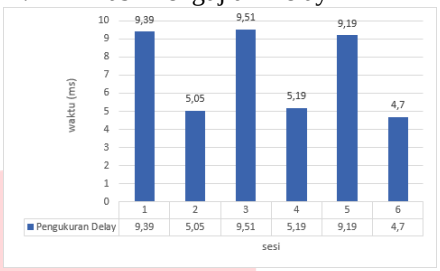


GAMBAR 4.
GRAFIK PENGUJIAN AVALANCHE EFFECT

Dari grafik diatas diketahui bahwa perbandingan dari Enkripsi AES 256 dan DES dengan variasi 5 huruf menghasilkan perbedaan yang signifikan. Dimana diketahui AES 256 memiliki Avalanche Effect dalam kategori bit yang baik dengan rata rata Avalanche Effect yaitu 51,5%. Namun dalam algoritma DES diketahui memiliki kategori yang dikatakan buruk yaitu melebihi dan kurang dari 45%-60% (yang merupakan kategori terbaik dari Avalanche Effect).

C. Hasil Pengujian Performansi Jaringan dengan Quality of Service

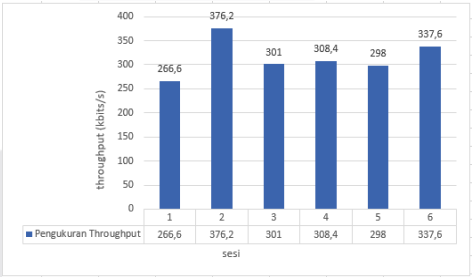
1. Hasil Pengujian Delay



GAMBAR 5.
GRAFIK PENGUJIAN DELAY

Skenario pengujian delay diatas menggunakan software Wireshark dengan memfilter paket data dari IP API server *heroku* dan TCP. Jumlah pengujian pengiriman dan pengambilan data ke API server dilakukan sebanyak 30 kali, yang dibagi menjadi 6 sesi yaitu 2 untuk pagi hari, 2 untuk siang hari, dan 2 untuk malam hari yang masing-masing sesinya terdiri dari 5 kali pengujian. Gambar diatas menunjukkan bahwa delay dari aplikasi android menuju API server memiliki nilai delay terkecil, delay rata-rata dan delay terbesar secara berurutan yaitu 4,7 s, 7,17 s dan 9,51 s.

2. Hasil Pengujian Throughput

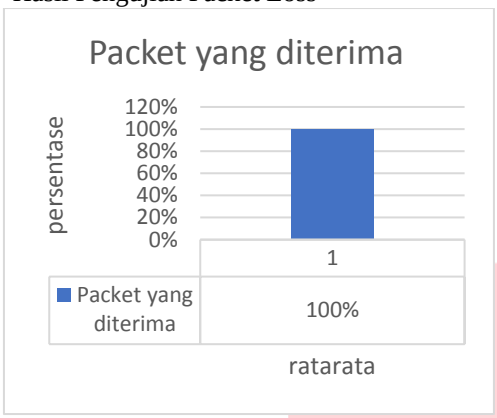


GAMBAR 6.
GRAFIK PENGUJIAN THROUGHPUT

Skenario Pengujian throughput menggunakan software Wireshark dengan cara memfilter paket data dari TCP. Jumlah pengujian pengiriman dan pengambilan data ke cloud server dilakukan sebanyak 30 kali, yang dibagi menjadi 6 sesi yaitu 2 untuk pagi hari, 2 untuk siang hari, dan 2 untuk malam hari yang masing-masing sesinya terdiri dari 5 kali pengujian. Gambar diatas menunjukkan rata-rata throughput dari aplikasi android ke API server sebesar 316,4 kbit/s dan bisa dikatakan baik. Hasil pengujian berbeda cukup signifikan karena kualitas dari koneksi internet yang tidak bisa

diprediksi, banyaknya pengguna jaringan, spesifikasi perangkat client dan spesifikasi server. Pengujian throughput dilakukan berbarengan dengan pengujian delay dengan dibagi menjadi 6 sesi.

3. Hasil Pengujian Packet Loss



GAMBAR 7.
GRAFIK PACKET YANG DITERIMA APLIKASI ANDROID

Dapat dilihat pada Gambar diatas bahwa jumlah paket yang berhasil dikirim dari sisi Aplikasi Android ke API Server kemudian paket yang berhasil diterima dari API Server menuju Aplikasi Android memiliki nilai sebesar 100%. Hal ini menandakan banyaknya paket yang hilang selama proses transmisi ke tujuan sebesar 0%. Dimana jumlah packet loss 0% dalam sistem yang dibuat memiliki performansi sangat baik pada skenario menggunakan jaringan Wi-Fi.

4. Black Box Testing

Hasil pengujian Black Box Testing pada 22 fitur di aplikasi android telah memenuhi ekspektasi dengan presentase keberhasilan program 100%.

IV. KESIMPULAN

1. Penelitian tugas akhir mengimplementasikan *Find Cataract System* berbasis android menggunakan algoritma *Advanced Encryption Standard* (AES) dan *Data Encryption Standard* (DES), yang mampu melakukan *inspect* mata pada pasien dan memberikan diagnosis keadaan mata.
2. Penelitian tugas akhir ini menggunakan algoritma AES-256 dan DES untuk mengamankan aplikasi *FCS*. Proses enkripsi pada aplikasi android ini terletak pada bagian registrasi data dan juga pada hasil inspect mata yang dikirimkan ke*firebase*. Berdasarkan pengujian yang dilakukan di dapatkan hasil *running-time*terbaik ada pada DES dengan rata-rata sekitar 0.0019 s, sedangkan untuk hasil tingkat keamanan *Avalanche effect* terbaik ada pada algoritma AES-256 dimana mendapatkan rata-rata *Avalanche effect* sekitar 51.5% dimana merupakan rentang terbaik dari pengujian tingkat keamanan *Avalanche effect*. Penelitian ini memilih AES-256 sebagai algoritma enkripsi untuk aplikasi FCS karena memiliki tingkat keamanan yang jauh lebih baik daripada DES. Walaupun untuk proses *running-time* algoritma ini lebih lama dibandingkan DES namun itu terjadi akibat keamanan round yang berlapis yang dilakukan oleh AES-256
3. Pada tugas akhir ini di lakukan pengujian pada durasi saat *user* melakukan scanning pada mata hingga diagnosa keluar. Rata-rata nilai yang di dapat adalah sebesar 2.8 s.
4. Berdasarkan pengujian *Quality of service* dari aplikasi android ke *API server Heroku* memiliki *delay* rata-rata 7.17 s dengan kategori *preferred* menurut standar ITU-IT, serta mendapatkan *throughput* 316,4 Kbps, dan *packet loss* 0% yang secara keseluruhan masuk kedalam kategori *preferred* standarisasi ITU-TG 1010. Skenario pengujian QOS ini dengan membagi pengujian menjadi 6 sesi dengan rentang pagi-siang-malam yang merupakan jam sibuk hingga jam senggang.

A. Saran

1. Membandingkan dengan algoritma enksripsi lain yang lebih baik.
2. Menggunakan metode lainnya dalam pengujian fungsionalitas aplikasi android seperti *White Testing* dan *running-time activity* serta menambah metode pengujian
3. Melakukan perhitungan durasi inspeksi mata menggunakan fungsi kodingan agar lebih akurat

REFERENSI

[1] A. N. Aini and Y. D. P. Santik, “Kejadian Katarak Senilis di RSUD Tugurejo,” *HIGEIA (Journal Public Heal. Res. Dev.*, vol. 2, no. 2, pp.

295–306, 2018, doi: 10.15294/higeia.v2i2.20639.

[2] A. F. Arifani, “Lensa dan Katara,” *J. Phys. Ther. Sci.*, vol. 9, no. 1, pp. 1–11,2018,[Online].Available:http://dx.doi.org/10.1016/j.neuropsychologia.2015.07.010%0Ahttp://dx.doi.org/10.1016/j.visres.2014.07.001%0Ahttps://doi.org/10.1016/j.humov.2018.08.006%0Ahttp://www.ncbi.nlm.nih.gov/pubmed/24582474%0Ahttps://doi.org/10.1016/j.gaitpost.2018.12.007%0Ahttps:

[3] Kementerian Kesehatan RI, “Infodatin (Situasi Gangguan Penglihatan Dan Kebutaan),” *Kementeri. Kesehat. RI*, vol. 53, no. 9, pp. 1689–1699, 2014.

[4] “PERDAMI – Perhimpunan Dokter Spesialis Mata Indonesia.” https://perdami.or.id/ (accessed Nov. 28, 2021).

[5] R.Juyel, G.Syed MD, “Cataract Detection Using Smartphone”, 7-9 Desember 2017. [online]. Available : https://sci-hub.se/10.1109/EICT.2017.8275136. [Accessed 2022].

[7] N. B. Tampubolon, R. R. Isnanto, and E. W. Sinuraya, “Implementasi Dan Analisis Algoritma Advanced Encryption Standard (Aes) Pada Tiga Variasi Panjang Kunci Untuk Berkas Multimedia,” *Transient J. Ilm. Tek. Elektro*, vol. 4, no. 4, pp. 1008–10112, 2016, doi: 10.14710/transient.4.4.1008-10112.

[8] K. Krosl *et al.*, “CatARact: Simulating Cataracts in Augmented Reality,” *Proc. - 2020 IEEE Int. Symp. Mix. Augment. Reality, ISMAR 2020*, pp. 682–693, 2020, doi: 10.1109/ISMAR50242.2020.00098.

[9] I. Erman, Y. Elviani, B. Soewito, D. Prodi, K. Lubuklinggau, and P. Kesehatan, “INSTALASI RAWAT JALAN (POLI MATA) RUMAH SAKIT DR . SOBIRIN KABUPATEN MUSI RAWAS TAHUN 2014,” 2014.

[10] P. Astari, “Katarak : Klasi kasi , Tatalaksana , dan Komplikasi Operasi,” vol. 45, no. 10, pp. 748–753, 2018.

[11] L. Penerbangan, A. Nasional, D. L. Penerbangan, A. Nasional, S. Pendeteksi, and H. Spasial, “DoubleClick : Journal of Computer and Information Technology Klasifikasi Data Radar (Ihsan) | 115 DoubleClick : Journal of Computer and Information Technology E-ISSN : 2579-5317 116 | Klasifikasi Data Radar ....(Ihsan),” vol. 4, no. 2, pp. 115–121, 2021.

[12] M. Ichwan, F. Hakiky, and J. T. Informatika, “Jurnal informatika,” vol. 2, no. 2, pp. 13–21.

[13] N. Monica, S. Sarkum, and I. Purnama, “Aplikasi Data Mahasiswa Berbasis Android: Studi Pada Sekolah Tinggi Ilmu Ekonomi Labuhanbatu,” *It J. Res. Dev.*, vol. 3, no. 1, pp. 43–53, 2018, doi: 10.25299/itjrd.2018.vol3(1).1849.

[14] B. Anwar, H. Jaya, P. I. Kusuma, P. Studi, and S. Komputer, "Issn : 1978-6603implementasi location based service berbasisandroid untuk mengetahuiposisi user," pp. 121–133, 1978.

[15] A. Kurniawan, *Network Forensics Panduan Analisis & Investigasi Paket Data Jaringan Menggunakan Wireshark*. Indonesia: ANDI, 2012.

[16] N. Saputro, "Kenali Pengertian Wireshark Beserta Fungsi dan Cara kerjanya, Lengkap!," *https://www.nesabamedia.com/pengertian-wireshark/*, 2019. .

[17] M. F. Adriant, I. Mardianto, J. T. Informatika, F. T. Industri, U. Trisakti, and T. Dasar, "IMPLEMENTASI WIRESHARK UNTUK PENYADAPAN (SNIFFING) PAKET DATA JARINGAN," pp. 224–228, 2015.

[18] Gerald Combs, "Wireshark," 2021. www.wireshark.org.

[19] D. B. Prasetyo, R. I. Miftah, and R. I. Perwira, *Manajemen Jaringan Menggunakan Firebase Cloud Massaging Berbasis Android*. LPPM UPN "Veteran" Yogyakarta, 2019.

[20] Firebase, "Firebase Brand Guidelines." https://firebase.google.com/brand-guidelines.

[21] A. A. Permana and D. Nurnaningsih, "RANCANGAN APLIKASI PENGAMANAN DATA DENGAN ALGORITMA ADVANCED ENCYPTION STANDARD (AES)," vol. 11, no. 2, 2018.

[22] B. K. Kriptografi, "Advanced Encryption Standard (AES)."

[23] Primartha Rifkie, "Penerapan Enkripsi dan Dekripsi File Menggunakan Data Encryption Standard (DES)," *ISNN 2355-4614 / Univ. Sriwij.*, vol. 3, no. 2, pp.371–387, 2011.

[24] Rasudin, "INTERNET DENGAN METODE HIERARCHY."

[25] K. Aziiz, M. A. Ineke Paekereng, " Perancangan Teknik Kriptografi Block CipherBerbasis Pola Batik Ceplok Yogyakarta" vol. 8, no.1 pp. 1-1