Cyber Attack Defense for Autonomous Rail Rapid Transit Safety

Dwi Nova Wijayanti (18217047)
Sistem dan Teknologi Informasi
Institut Teknologi Bandung
dwinovawijayanti@yahoo.co.id

***Abstrak*— Menurut rancangan ibukota baru oleh Pemerintah Republik Indonesia, akan digunakan teknologi *autonomous rail rapid transit* sebagai alat transportasi massal utama di ibukota baru. *Autonomous rail rapid transit* merupakan kendaraan pintar tanpa pengemudi yang bergerak menggunakan sensor *hi-tech* untuk mengumpulkan informasi perjalanan dan mengidentifikasi trotoar serta benda-benda lain yang ada di jalanan. Penggunaan *high technology* ini tentunya memiliki ancaman risiko keamanan tersendiri, terlebih lagi *autonomous rail rapid transit* ini berskala besar dan akan digunakan untuk ibukota negara. Keamanan informasi kendaraan ini tentunya menjadi hal yang krusial untuk dijaga agar tidak terjadi kecelakaan-kecelakaan yang berakibat fatal.**

Kata kunci—autonomous rail rapid transit, hi-tech, sensor, cyber attack

I. PENDAHULUAN

1.1 Latar Belakang

Pada dewasa ini, teknologi kian berkembang dengan pesat, segala hal yang awalnya konvensional kini mulai beralih ke arah digital. Perkembangan teknologi ini bahkan tidak terbatas lagi dan telah menyebar ke berbagai sektor baik sektor ekonomi, industri maupun sektor transportasi. *Smart city* saat ini sedang digemari oleh ahli-ahli teknologi, mencari solusi untuk dapat memanfaatkan segala sumber daya yang dimiliki disuatu negara agar kehidupan di dalamnya menjadi sangat efisien. Sektor transportasi menjadi salah satu fokus ahli teknologi untuk menciptakan *smart city*.

Pemerintah Indonesia merencanakan ibukota baru menjadi kota pertama di Indonesia yang akan menjadi *smart city*. Kota tersebut akan menjadi kota termaju di Indonesia dengan penggunaan teknologi di setiap sisinya. Berkaca dari Negara Cina yang telah berhasil menjadikan *autonomous rail rapid transit* sebagai alat transportasi publiknya,

Pemerintah Indonesia juga akan menggunakan *autonomous rail rapid transit* atau ART di ibukota baru.

Autonomous rail rapid transit ini menggunakan beberapa *high* technology dalam pembuatannya. Penggunaan teknologi dalam skala besar ini tentunya memiliki risiko yang besar juga terutama dari segi keamanannya. Pencegahan penyerangan siber dalam sistem informasi tentu harus direncanakan sebaik mungkin karena ini menyangkut kehidupan masyarakat di kota tersebut.

1.2 Rumusan Masalah

Sehubungan dengan latar belakang yang telah dijelaskan sebelumnya, rumusan masalah yang diangkat pada makalah ini adalah sebagai berikut.

1. Bagaimana sistem yang digunakan oleh *autonomous rail rapid transit*?
2. Bagaimana *cyber-attack* yang dilakukan terhadap sistem dan akibatnya?
3. Bagaimana cara mempertahankan keamanan informasi sistem *autonomous rail rapid transit* dari penyerangan siber?

1.3 Tujuan Makalah

Makalah ini bertujuan untuk menjelaskan salah satu alat transportasi publik yaitu *autonomous rail rapid transit* yang akan digunakan pada ibukota baru Indonesia dari segi sistem informasi dan keamanannya.

II. LANDASAN TEORI

2.1 Autonomous Rail Rapid Transit

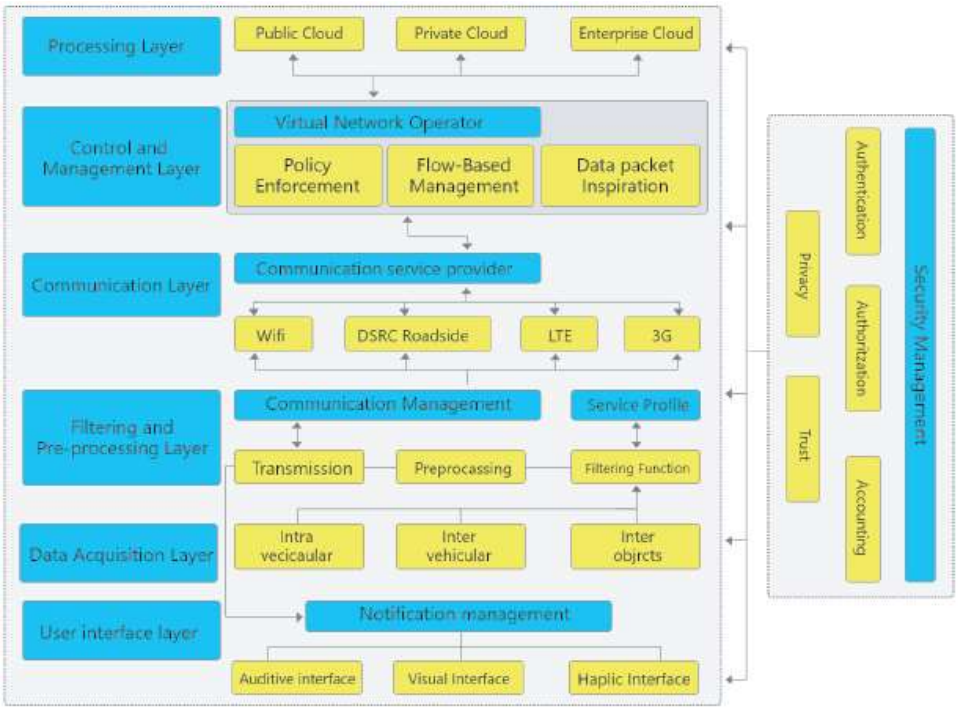
Dipublikasikan pertama kali pada 2 Juni 2017 di Zhuzhou, Provinsi Hunan, China, *autonomous rail rapid transit* ini adalah alat transportasi listrik cerdas yang merupakan persilangan antara bus, kereta dan trem yang mengimplementasikan Internet of Autonomous Vehichle (IoAV). ART ini berjalan menggunakan ban karet dengan orbit virtual berupa dua garis putih yang terpasang pada jalan raya. Terdapat sistem sinyal pada setiap stasiun dan sensor yang dapat mengukur dimensi jalan raya yang dilewatinya.

Autonomous rail rapid transit ini dijalankan menggunakan energi listrik dan mampu berjalan sejauh 25 kilometer setelah di-*charge* selama 10 menit. Alat ini juga dilengkapi dengan kamera 360^{o} dan radar untuk proteksi keamanan dari berbagai benda yang berada di sekitarnya. Terdapat sebuah *blackbox* yang berfungsi sebagai sistem interkom untuk komunikasi dengan penumpang dan CCTV untuk pengawasan dari pusat kontrol sistem. Sistem *wireless communication* digunakan antara *autonomous rail rapid transit* dengan pusat kontrol sistem. Roda karet menjadi elemen utama pada *autonomous rail rapid transit* ini karena digunakan teknologi khusus yang diintegrasikan dengan trek virtual sebagai penunjuk jalan otomatis.

2.2 Internet of Autonomous Vehicle

Sebelumnya telah disinggung mengenai IoAV di *autonomous rail rapid transit*, disini akan dibahas konsep fundamental dari IoAV terlebih dahulu. *Internet of Autonomous Vehicle* (IoAV) adalah evolusi terbaru dan ekspansi dari *Internet of Things* (IoT) [1]. Seperti yang diketahui, *Internet of Things* adalah salah satu teknologi terkemuka saat ini dan terus melakukan perkembangan ke berbagai bidang yang lebih spesifik. Salah satunya adalah VANET atau *Vehicular Ad hoc Network* yang berfokus pada sistem komunikasi antar kendaraan dan infrastruktur. Sistem komunikasi eksternal adalah sistem yang kompleks karena topologi yang sangat dinamis seperti kecepatan kendaraan, mobilitas, komunikasi nirkabel dalam medium terbuka, tidak adanya sistem keamanan yang tetap serta banyaknya jumlah kendaraan yang berada di jalan. Secara umum, komunikasi dalam VANET dikelompokkan menjadi 2 jenis; *Vehicle to*

Vehicle (V2V) dan dan *Vehicle to* RSU (V2R). *Vehicle to Vehicle* adalah komunikasi nirkabel yang diciptakan antarkendaraan otonom, untuk kasus ini komunikasi yang dimaksud adalah komunikasi antar *autonomous rail rapid transit* dalam satu kota. *Vehicle to* RSU adalah komunikasi informasi dari kendaraan dengan *Road Side Unit* (RSU) untuk pemantauan dan layanan pengelolaan [2]. Jaringan kendaraan utama terdiri atas sistem komunikasi antarkendaraan dengan berbagai sensor pendukung untuk pengumpulan data-data.



Gambar 1 Struktur Arsitektur Berlapis IoAV

(sumber : https://ieeexplore.ieee.org/document/8809661)

Struktur arsitektur *internet of autonomous vehicle* terdiri atas 6 lapisan [1]:

1.) Lapisan *user interface* sebagai media interaksi antara kendaraan dengan pengguna. Biasanya memberikan informasi notifikasi penting terkait kendaraan kepada pengguna.
2.) Lapisan *data acquisition* berperan sebagai penerima dan pengumpul data-data dari berbagai sensor sebagai *input* dalam proses selanjutnya

3.) Lapisan *filtering and pre-processing*, di lapisan ini data yang telah dikumpulkan dari berbagai sensor dianalisis dan disaring menjadi data-data yang relevan dengan kebutuhan kendaraan

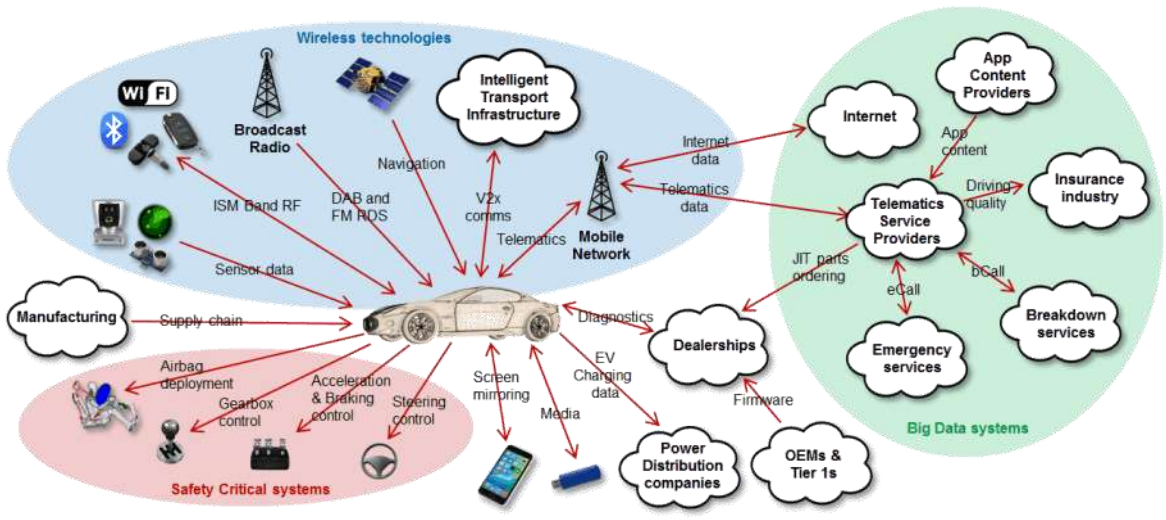
4.) Lapisan *communication* ini memilih medium transmisi data-data yang terbaik dengan menganalisis beberapa parameter seperti kualitas, keamanan, privasi dan reliabilitas.

5.) Lapisan *control and management* berfokus pada pengendalian dan pengelolaan kebijakan penyedia layanan jaringan

6.) Lapisan *processing* bertanggungjawab dengan urusan infrastruktur *cloud* yang menerima data yang sangat banyak dari berbagai kendaraan untuk diproses lebih lanjut dan disalurkan ke aplikasi terkait.

III. JENIS – JENIS PENYERANGAN SIBER PADA *AUTONOMOUS RAIL RAPID TRANSIT*

Penggunaan teknologi dalam segala aspek menjadi tantangan baru bagi pengembang *autonomous rail rapid transit* sebab setiap elemen memiliki risiko tersendiri. Penyerangan siber pada alat transportasi umum ini dapat dilakukan dari beberapa bagian inti seperti GPS, LiDAR, *wireless network* dan kamera.



Gambar 2 Penyerangan siber dari berbagai arah

(sumber : https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/august/uk-government-cyber-security-guidelines-for-connected-and-autonomous-vehicles/)

3.1 Penyerangan Siber pada Jaringan Sensor

Persepsi sensor adalah proses perubahan lingkungan fisik sekitar kendaraan menjadi sinyal digital untuk diproses lebih lanjut. Jaringan sensor adalah target yang menarik bagi penyerang, khususnya serangan eksternal yang terbatas pada masukan melalui saluran *input* dan *output* seperti *Bluetooth, keyless entry systems* dan port pemeliharaan nirkabel [3]. Biasanya sensor yang digunakan adalah sensor ultrasonik, yang mengtransmisikan gelombang suara (50 KHz) dan memantulkannya kembali untuk menghitung jarak objek dari kendaraan.

3.2 Penyerangan Siber pada Kamera

Penggunaan kamera pada *autonomous rail rapid transit* cukup banyak, baik untuk pemantauan penumpang, lingkungan sekitar kendaraan, laju jalur dan informasi jalan raya. Data-data ini akan dikirimkan sebagai sinyal video digital ke pusat kontrol. Penyerangan pada kamera biasanya dilakukan dengan pengubahan gambar dari informasi jalan raya seperti perubahan rambu lalu lintas.

3.3 Penyerangan Siber pada GPS

Pada zaman ini siapa yang tidak mengetahui GPS. GPS atau *global positioning systems* menyediakan layanan sinkronisasi lokalisasi dan waktu menggunakan jaringan internet. Data GPS mentransmisikan kode *coarse* / *acquisition* (C/A) dengan *pseudorandom noise* (PRN) nya sendiri. Ada beberapa metode untuk sistem satelit navigasi global mendapatkan perkiraan lokasi yang baik; pertama. Sistem augmentasi berbasis satelit (SBAS), Assisted-GPS (AGPS) dan Differential-GPS (DGPS). SBAS umumnya digunakan di pesawat terbang, untuk fase kritis seperti fase pendaratan. Menurut Raiyn, keakuratan posisi dipengaruhi oleh faktor-faktor eksternal seperti cuaca luar angkasa. Selain itu, jika sinyal satelit mencapai bumi, itu dapat dipantulkan dari bangunan dan benda lain, menyebabkan peningkatan waktu tempuh dan mempengaruhi pengukuran [4].

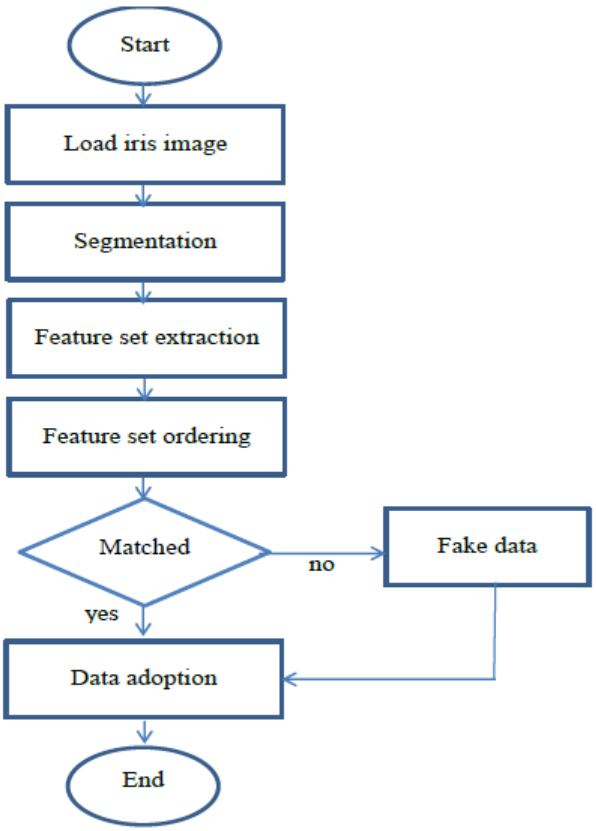
3.4 Penyerangan Siber pada *Light Detection and Ranging* (LiDAR)

Light Detection and Ranging atau juga biasa disebut *Laser Distance Sensor* melibatkan jenis sensor penemuan jangkauan. Berbeda dengan sensor ultrasonik, LiDAR memancarkan gelombang cahaya dan mengukur waktu yang diperlukan untuk gelombang dapat memantul kembali dari suatu permukaan yang jauh. LiDAR hanya mampu mengukur jarak objek-objek yang bergerak cepat seperti kendaraan di jalan raya dan cocok digunakan untuk mengukur permukaan objek kecil lainnya. Konsep LiDAR adalah melihat objek yang memantulkan sinya, jika sinyal gagal kembali baik dikarenakan penyerapat, objek transparan ataupun karena batas jangkauan, maka sistem menyimpulkan tidak ada objek. Penyerangan yang dilakukan pada LiDAR adalah *replay attack*, yaitu mengirimkan sinyal asli sistem LiDAR kendaraan yang ditargetkan dari posisi lain untuk membuat gema palsu.

IV. Model Sistem dan Target Keamanan

Dalam makalah ini, sistem yang digunakan untuk menjaga keamanan *autonomous rail rapid transit* adalah dengan enkripsi biometri. Enkripsi biometrik pada umumnya digunakan untuk tujuan otentikasi. Karakteristik fisiologis seseorang seperti sidik jari dan iris merupakan fitur-fitur yang unik dan mampu membedakan seseorang. Pada kali ini, akan digunakan data biometrik menggunakan pengenalan iris.

Metodologi pengenalan iris terbagi atas dua fase; *training* dan *testing*. *Training*, pada fase ini, sistem akan mempelajari fitur-fitur dari sebuah iris dan dilakukan optimasi pada algoritma *training* secara terus menerus. *Testing*, sistem melakukan pengujian terhadap algoritma yang telah dikembangkan dengan masukan data-data biometrik yang terdapat pada *database*. Pada gambar 3 di bawah ini adalah alur *testing* dari pengenalan sebuah iris. Mula-mula gambar iris pada *database* dimuat ke sistem, lalu masuk ke proses segmentasi, yaitu mendeteksi kelopak mata atas dan bawah serta batas pupil dan iris. Kemudian fitur-fitur unik yang terdapat pada iris diekstrak untuk disimpan (dipelajari oleh mesin). Dilakukan pencocokan vector dalam bentuk kode biner berdasarkan algoritma *minimum hamming distance*. Hasil yang dikeluarkan oleh sistem adalah diterima atau ditolak berdasarkan hasil pencocokan sebelumnya.



Gambar 3 Flowchart Pengenalan Iris

(sumber : https://www.researchgate.net/publication/329419711_Data_and_Cyber_Security_in_Autonomous_Vehicle_Networks)

Pada sistem ini digunakan algoritma *Identification and Detection Unit* (IDU) untuk memprediksi hasil keluaran. Algoritma IDU digunakan untuk pendeteksi warna dari gambar mata baik dalam format analog maupun digital. Objek-objek yang terdeteksi dipecah dalam beberapa *frame* yang terdiri dari sekumpulan pixel. *Database* yang digunakan terbagi dua; *training* dan *testing.* Contoh di bawah ini adalah visualisasi *frame* dari suatu data pada *training database*.

$$X_1 = \{x_1^1, x_2^1, \ldots, x_n^1\}$$
$$X_2 = \{x_1^2, x_2^2, \ldots, x_n^2\}$$
$$\ldots\ldots$$
$$X_n^m = \{x_1^m, x_2^m, \ldots, x_n^m\}$$

Pada makalah ini *training database* sebagai X dan *testing database* sebagai Y. Untuk menghitung nilai faktor korelasi, digunakan algoritma IDU dan *database* yang telah disediakan. Perhitungan faktor korelasi menggunakan metode statistika XOR.

$$J = X \oplus Y$$

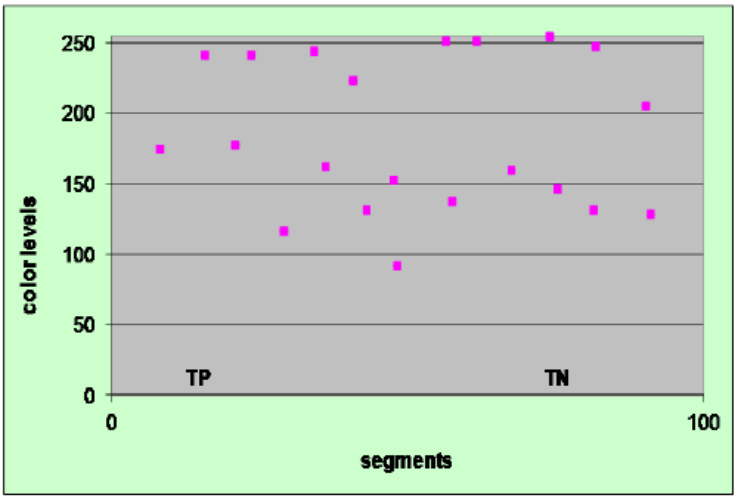
$$J = \begin{cases} 1 & \text{if } x \neq y \\ 0 & \text{otherwise} \end{cases}$$

$$\underbrace{\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}}_{segements} XOR \underbrace{\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}}_{\text{Data Set}}$$

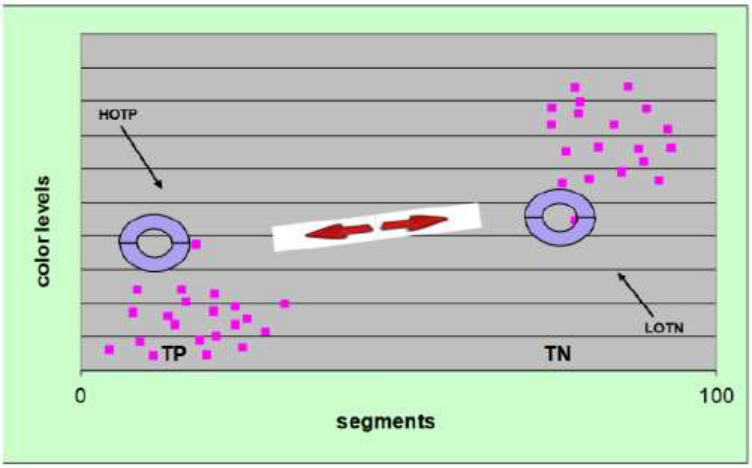
Berikut ini adalah rumus optimisasi dari nilai faktor korelasi:

$$J_{\Pr ediction}(J_1^*) = J_{demand} + k^*(\Delta J)$$

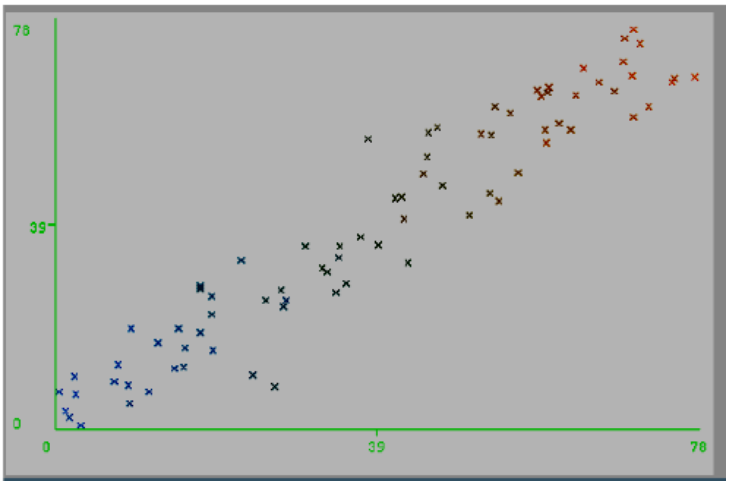
Berikut ini adalah contoh ilustrasi implementasikan ke dalam sistem. (*Disclaimer*: percobaan ini tidak dilakukan oleh penulis melainkan hasil percobaan yang diambil dari jurnal referensi [3] yang telah dibaca penulis).



Gambar 4 Level Warna



Gambar 5 Klasifikasi warna



Gambar 6 Level warna dalam gambar

Untuk menjaga keamanan data privasi biometric ini, terdapat beberapa teknik proteksi yang dikembangkan berdasarkan enkripsi biometrik seperti *fuzzy commitment*, *fuzzy fault*, *fuzzy extractor* dan *unified abstraction*[5].

1. *Fuzzy commitment*

   Pada tahap pendaftaran data biometric, rumus $\alpha = bk - bio$ dihasilkan secara otomatis, dimana *bk* menggambarkan kunci acak dan *bio* adalah sampel biometric. Pada tahap verifikasi, terdapat sampel lain *bio'* dan nilai *bk* menjadi $f(\alpha+bio') = f(bk+ (bio' - bio))$ dimana *f* adalah fungsi koreksi kesalahan. Jika selisih *bio'* dengan *bio* kurang dari kapasitas δ, maka nilai *bk* dapat dipulihkan.
2. *Fuzzy vault*

Pada tahap pendaftaran data biometric dihasilkan polynomial berdasarkan kunci acak *bk*, dan sampel biometric diproyeksikan dalam bentuk poin. Pada tahap verifikasi, terdapat sampel biometric lain *bio'*, polynomial dapat dihasilkan kembali jika sebagian besar *bio'* tumpang tindih dengan *bio* (hampir serupa), dan nilai *bk* dapat dipulihkan.

3. *Fuzzy extractor*

   Pada tahap pendaftaran, sampel biometric *bio* digunakan sebagai masukan yang dapat men-*generate* kunci rahasia *bk* dan sebuah *string* tambahan *aus*. Pada tahap verifikasi, *bk* dapat di ekstrak dari *aus* dan sampel biometric lain *bio'* hanya jika *bio* dan *bio'* menyukupi perkiraan.

4. *Unified abstraction*

   Pada abstraksi ini, terdapat dua algoritma utama yang dapat melakukan pendekatan perlindingan privasi biometric. *BIO* menggambarkan fitur biometric tertentu.

   (*bk, tp)* ← *KeyTPGen(bio)* : kunci probabilitas dan algoritma pembuatan template *tp*, dengan masukan sampel biometrik *bio* ϵ *BIO.*

   bk' ← *KeyRel(tp,bio')* : algoritma pelepasan kunci deterministic dengan masukan template *tp* dan sampel biometric *bio'* dan keluaran kunci *bk'.* Nilai *bk'* dan *bk* akan sama jika *bio* dan *bio'* menyukupi perkiraan.

V. KESIMPULAN

Aspek keamanan dalam kendaraan cerdas bukanlah suatu tantangan yang mudah. Terdapat banyak celah dalam sistem informasi *autonomous rail rapid transit* yang menjadi sasaran penyerangan. Penyerangan siber pada sistem informasi *autonomous rail rapid transit* akan berakibat fatal dan mengancam nyawa banyak orang yang menaikinya. Setiap inovasi teknologi yang digunakan harus memiliki strategi tersendiri dalam menjaga data informasinya. Melalui data biometrik seperti iris yang bersifat unik pada setiap orang, proses otentikasi sistem menjadi lebih akurat dan terjamin. Jaringan komunikasi nirkabel pada *autonomous rail rapid transit* dapat terjaga dengan baik sehingga dapat beroperasi dengan lancar tanpa gangguan.

Referensi

[1] A. Nanda, D. Puthal, J. J. P. C. Rodrigues and S. A. Kozlov. "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions," in IEEE Wireless Communications, vol. 26, no. 4, pp. 60-65, August 2019.

[2] K. M. Ali Alheeti and K. McDonald-Maier. "An intelligent security system for autonomous cars based on infrared sensors," 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, 2017, pp. 1-5.

[3] Raiyn, J. (2018). Data and Cyber Security in Autonomous Vehicle Networks. *Transport and Telecommunication Journal, 19*, 325 - 334.

[4] Khayyam, Hamid & Javadi, Bahman & Jalili, Mahdi & Jazar, Reza. (2020). Artificial Intelligence and Internet of Things for Autonomous Vehicles.

[5] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma and K. R. Choo, "Unified Biometric Privacy Preserving Three-factor Authentication and Key Agreement for Cloud-assisted Autonomous Vehicles," in IEEE Transactions on Vehicular Technology.

[6] Y. Yang, H. Lu, J. K. Liu, J. Weng, Y, "Credential Wrapping: From Anonymous Password Authentication to Anonymous Biometric Authentication," in Proc. AsiaCCS, 2016, pp. 141–151.

[7] V.LL. Thing, dan J. Wu. "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences". presented at the IEEE Intenational Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 15-18 Dec., 2016

[8] S. Zhao, J. Dang and H. Ma, "Research of China high-speed train transport operation system based on autonomous integration," 2009 International Symposium on Autonomous Decentralized Systems, Athens, 2009, pp. 1-5.

[10] Yağdereli, E., Gemci, C., & Aktaş, A. Z. (2015). A study on cyber-security of autonomous and unmanned vehicles. The Journal of Defense Modeling and Simulation, 12(4), 369–381.

[11] H. G. Garakani, B. Moshiri and S. Safavi-Naeini, "Cyber Security Challenges in Autonomous Vehicle: Their Impact on RF Sensor and Wireless Technologies," 2018 18th International Symposium on Antenna Technology and Applied Electromagnetics (ANTEM), Waterloo, ON, 2018, pp. 1-3.