Computatio: Journal of Computer Science and Information Systems, 8/1 (2024), 104 - 109

PENERAPAN KLASIFIKASI SUARA SEBAGAI AUTENTIKASI KEAMANAN SISTEM LOGIN MENGGUNAKAN GAUSSIAN MIXTURE MODELS

Audie Milson[1], Dyah Erny Herwindiati[2], Novario Jaya Perdana[3]
Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Tarumanagara,
Jln. Letjen S. Parman No. 1, Jakarta, 11440, Indonesia
E-mail: [1]audie.535180021@stu.untar.ac.id, [2]dyahh@fti.untar.ac.id, [3]novariojp@fti.untar.ac.id

Abstrak

Program penerapan klasifikasi suara sebagai auntetikasi keamanan sistem login merupakan sebuah program berbasis website yang dibuat untuk menguji efektivitas metode autentikasi suara sebagai alternatif metode autentikasi biometrik dalam meningkatkan keamanan sistem login suatu aplikasi. Program website yang dibuat terdiri dari bagian Frontend dan bagian Backend yang dibangun dengan modul Python Flask dalam pembentukan API yang berfungsi sebagai fungsionalitas website dan modul Vue Js dalam pembuatan tampilan aplikasi. Aplikasi yang dibuat kemudian diuji dari segi fungsionalitas, tingkat akurasi model dalam mengklasifikasikan suara dan keamanannya dengan metode blackbox testing dan serangkaian security test seperti penetration testing, SQL Injection, dan XSS Attack dengan hasil pengujian aplikasi berfungsi sesuai ekspektasi dan tidak rentan terhadap serangan SQL Injection ataupun XSS Attack, sedangkan hasil dari pengujian tingkat akurasi model dalam mengklasifikasikan suara menghasilkan tingkat akurasi sebesar 67% dengan menggunakan 5 suara sebagai input awal. Hasil dari serangkaian pengujian yang telah dilakukan menunjukan bahwa perpaduan metode Linear Predictive Coding dan Gaussian Mixture Model kurang efektif dalam mengklasifikasikan suara, akan tetapi metode Autentikasi Suara berhasil meningkatkan tingkat keamanan sistem login pada aplikasi.

Kata kunci—*Login, GMM, Linear Predictive Coding, Autentikasi Suara*

Abstract

The Implementation of Voice Classification as Login System Authentication Program is web based application designed to measure the effectiveness of voice authentication method as one of biometrics authentication alternative on the context of increasing an app login system security. The application created is divided into two parts namely Frontend and Backend, the frontend part is created with VueJs Framework and the backend part is created in the form of API with Python Flask Module. The Application created then tested with blackbox testing, voice classification model perfomance and Security test such as Penetration Testing, SQL Injection, and XSS Attack. The results obtained are in the form of program vulnerability analysis against SQL Injection and XSS Attack, but in terms of Model Perfomance the voice classification model can performs user identification with 67% accuracy using 5 voices as initial input. Based on blackbox testing results, security test results, and Model performance accuracy test "The Implementation of Voice Classification as Login System Authentication using Gaussian Mixtures Model" conclude that the combination of Linear Predictive Coding Method and Gaussian Mixture Model are not effective on voice classification, but voice authentication method successfully increase an app login system security.

Keywords—*Login, GMM, Linear Predictive Coding, Voice Authentication*

1. PENDAHULUAN

Pandemi Covid-19 telah merubah banyak hal mulai dari tata cara bekerja bahkan hingga perubahan pola gaya hidup yang sekarang berubah menjadi digital, perubahan yang terjadi tentu berdampak baik dengan terakselerasinya perkembangan teknologi namun juga memunculkan permasalahan yang semakin marak terjadi yaitu serangan siber. Serangan Siber yang marak terjadi berupa XSS Attack, SQL Injection, dan Weak Password [3].

Berdasarkan permasalahan Serangan Siber yang ada, banyak solusi yang telah digunakan untuk mengurangi potensi terjadinya serangan siber yaitu dengan menerapkan mekanisme autentikasi ganda pada sistem login aplikasi. Salah satu metode autentikasi yang paling efektif yaitu metode autentikasi biometrik yang umumnya menggunakan biometrik sidik jari ataupun retina mata akan tetapi kedua biometrik tersebut memerlukan perangkat tambahan dengan biaya yang tergolong tinggi karena itu dibutuhkan metode autentikasi biometrik alternatif yang tidak memerlukan perangkat khusus dengan harga tinggi yaitu metode autentikasi biometrik suara.

Dalam upaya membuat metode autentikasi biometrik suara ini menjadi lebih umum di semua industri maka perlu dibuatnya *Application Programming Interface* (API) yang dapat memproses dan mengklasifikasikan data biometrik suara pengguna yang nantinya dapat digunakan pada sistem login aplikasi manapun yang menghubungkan program backend aplikasi dengan API Autentikasi Biometrik Suara.

Jurnal ini membahas mengenai efektivitas API Autentikasi Biometrik Suara dalam mengklasifikasikan suara pengguna dan meningkatkan tingkat keamanan sistem login pada aplikasi yang menerapkan autentikasi biometrik suara. Penerapan Autentikasi Biometrik Suara digunakan sebagai autentikasi tambahan setelah pengguna berhasil melewati autentikasi dengan password.

2. METODE PENELITIAN

2.1 Data

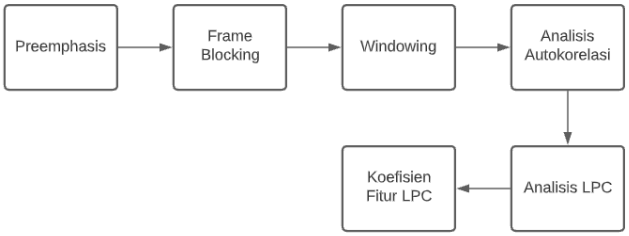
Data yang digunakan dalam penerapan klasifikasi suara sebagai autentikasi keamanan sistem login menggunakan *Gaussian Mixture Models* adalah data suara yang diperoleh melalui *Google Form* dalam bentuk file suara dengan ekstensi wav. Data suara yang diperoleh adalah sebanyak 5 file suara untuk setiap responden dengan total jumlah file suara yang didapatkan sebanyak 150 file suara, Data yang digunakan adalah data yang terkumpul selama periode pengumpulan file suara dari tanggal 17 Agustus 2021 sampai 20 November 2021.

2.2 *Preprocessing Data*

Data yang telah dikumpulkan kemudian dibagi menjadi dua bagian dengan rasio 80:20 untuk Data yang digunakan sebagai data latih dan data yang digunakan sebagai data uji. Pemilihan rasio yang didapatkan setelah melakukan beberapa percobaan terhadap keseluruhan data. Tujuan dari pembagian data menjadi data latih dan data uji adalah untuk menentukan performa model dan tingkat akurasi model dalam mengklasifikasikan data suara. Setelah pembagian data dilakukan tahap pra-pemrosesan data suara dilakukan dengan mengolah data suara menjadi data yang dapat diproses pada tahap selanjutnya. Data suara yang telah diproses menjadi bentuk vektor numerik kemudian dilakukan proses ekstraksi ciri fitur suara dengan Teknik *Linear Predictive Coding* (LPC). Ciri fitur suara yang diekstraksi pada Teknik LPC dilakukan dengan menormalisasi sinyal digital sehingga menghasilkan koefisien Fitur suara.

2.3 *Linear Predictive Coding*

Linear Predictive Coding (LPC) merupakan sebuah teknik analisis ucapan yang dapat digunakan untuk mengekstraksi fitur suara yang efisien untuk komputasi, Pada dasarnya cara kerja Teknik LPC yaitu melakukan analisis dengan memprediksi intensitas dan frekuensi sinyal suara [6]. Tahapan ekstraksi fitur suara menggunakan Teknik LPC dapat dilihat pada Gambar 1.



Gambar 1 Diagram Alur Teknik LPC

2.4 *Gaussian Mixture Model*

Gaussian Mixture Model (GMM) merupakan algoritma untuk memodelkan sejumlah data menjadi sebuah distribusi gaussian dengan parameter mean dan variance tertentu, dimana mean atau rata – rata bereperan sebagai titik pusat distribusi gaussian dan variance berperan sebagai ukuran persebaran nilai pada set data, GMM sendiri merupakan model statistic dari distribusi probabilitas nilai bobot setiap gaussian sehingga GMM merupakan metode yang sangat tepat baik dengan parameter ataupun tidak [1].

$$g(x|\mu_i, \Sigma_i) = \frac{1}{(2\pi)^{D/2}|\Sigma_i|^{1/2}} exp \ -\frac{1}{2}(x - \mu_i)' \sum_{i=1}^{M}(x - \mu_i) \quad (1)$$

2.4.1 *Expectation-Maximization*

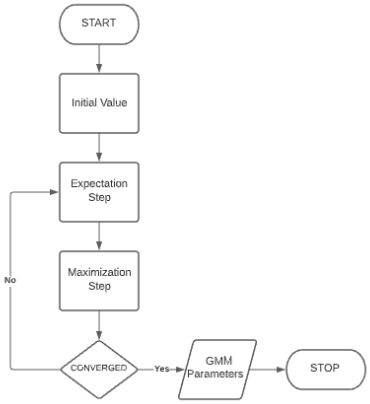
Penerapan algoritma Gaussian Mixture Model dapat dilakukan dengan menerapkan algoritma *Expectation Maximization* (EM), algoritma EM menggunakan data yang ada untuk menentukan nilai optimal dari variabel dan kemudian menentukan parameter model, Algoritma EM terdiri dari dua tahap yaitu tahap Ekspektasi untuk melakukan estimasi nilai dan variabel yang hilang atau belum ada dan tahap Maksimisasi untuk memperbarui parameter dengan menggunakan nilai yang didapatkan pada proses ekspektasi dah tahapan ini dilakukan secara terus menerus hingga menemukan titik konvergen dan menemukan maximum likelihood [4].

$$E\left[z_{i,j}\,|\mu^k\right] = \frac{\lambda_j L(x_i|\mu = \mu_j^k)}{\Sigma_i \lambda_j L(x_i|\mu = \mu_j^k)} \quad (2)$$

$$\mu_j^{k+1} = \frac{\Sigma_i E\left[Z_{i,j}|\mu^k x_i\right]}{\Sigma_i E\left[Z_{i,j}|\mu^k\right]} \quad (3)$$

$$L[x_i|\mu^k] = \Sigma_j \lambda_j L(x_i|\mu = \mu_j^k) \quad (4)$$

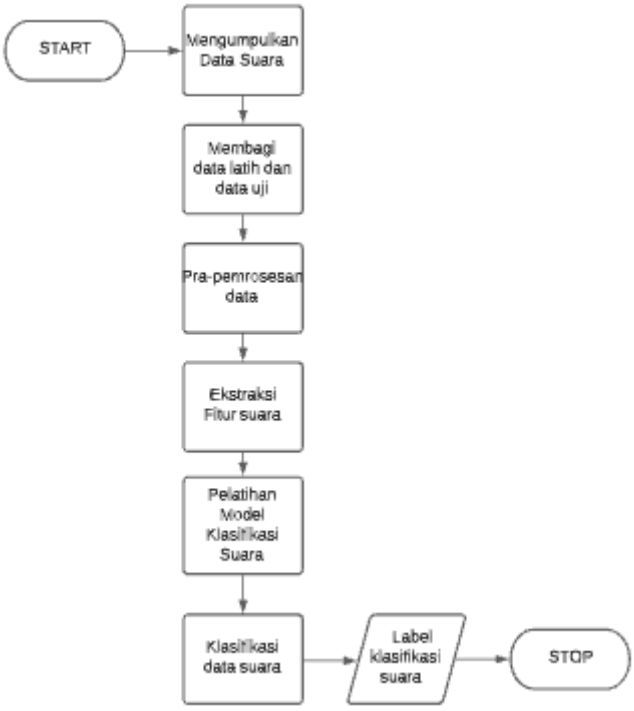
Dengan tahapan di atas proses pembentukan model GMM dengan algoritma EM dilakukan dengan tahap inisialisasi, tahap Ekspektasi, dan kemudian dilanjutkan ke tahap Maksimisasi, kemudian terdapat proses perhitungan *likelihood* dan proses dilanjutkan secara terus menerus hingga nilai *likelihood* sudah konvergen dan tidak mengalami perubahan lagi. Diagram alur proses pembentukan model GMM dapat dilihat pada Gambar 2.



Gambar 2 Diagram Alur Proses GMM

2.5 Rancangan Percobaan

Berikut merupakan diagram alur rancangan percobaan yang akan berjalan, dapat dilihat pada Gambar 3 berikut ini.



Gambar 3 *Diagram Alur percobaan klasifikasi suara*

Berdasarkan pada Gambar 3, tahapan yang perlu dilakukan dalam pembentukan model klasifikasi suara diawali proses pengumpulan data suara, dan kemudian membagi data suara yang telah dikumpulkan menjadi data latih dan data uji. Setelah data telah dibagi sesuai proporsi data latih dan data uji yang ditentukan, data kemudian dilakukan pra-pemrosesan terlebih dahulu sebelum melanjutkan ke tahap selanjutnya.

Data yang telah melalui tahap pra-pemrosesan kemudian diproses ekstraksi fiturnya dengan menerapkan teknik LPC dan menghasilkan data dalam bentuk vektor numerik yang akan digunakan sebagai data latih pada model GMM dengan hasil klasifikasi berupa label pada data suara yang diproses.

2.6 *Penetration Testing*

Penetration Test merupakan sebuah praktik secara aktif yang digunakan untuk menilai pertahanan jaringan komputer dengan merencanakan dan mengeksekusi semua kemungkinan serangan untuk mengeksploitasi kerentanan yang ada dengan tujuan menilai dan mencari potensi kerentanan pada sistem yang ada [2].

2.7 SQL Injection

SQL Injection merupakan sebuah metode pengujian ketahanan sistem yang dilakukan dengan mempengaruhi query SQL yang dikirimkan melalui aplikasi ke *database*, pengujian dilakukan dengan tujuan untuk mengurangi dan mencegah serangan injeksi pada aplikasi dengan menentukan metode pencegahan yang tepat.

2.8 XSS Attack

XSS *Attack* atau *Cross Site Scripting* merupakan bagian dari serangan injeksi yang secara sederhana dilakukan dengan menginjeksi kode yang biasanya berupa script yang dapat dieksekusi pada browser, pada umumnya jenis serangan ini digunakan untuk mencuri data identitas pengguna lainnya menggunakan cookies, session token, dan informasi lainnya [5].

3. HASIL DAN PEMBAHASAN

Percobaan dilakukan dengan mengumpulkan data suara melalui *Google Form* dengan menyebut format kalimat pengenalan diri pemilik suara. Data suara yang dikirimkan pada *Google Form* pengumpulan suara merupakan suara yang direkam menggunakan perangkat masing – masing responden dengan kriteria perekaman sebanyak 5 kali per responden dengan durasi minimal 5 detik, hasil perekaman suara berupa file data suara dengan format WAV.

Hasil pengumpulan data suara yang berhasil dikumpulkan sejumlah 150 file suara yang diperoleh dari 30 responden, kemudian data suara yang dikumpulkan akan diinput pada menu registrasi aplikasi yang dibuat tujuannya agar data dari setiap responden pengumpulan file suara dapat dipetakan antara akun pengguna beserta detail informasi data suara masing – masing pengguna. Setelah data akun pengguna dan detail informasi data suara pengguna dipetakan, maka proses selanjutnya yaitu membagi data suara yang telah dikumpulkan menjadi dua bagian yaitu data latih dan data uji dengan rasio 80:20 dengan tujuan mengukur performa model dalam mengklasifikasikan suara.

Proses pembentukan model klasifikasi suara dimulai dengan mengolah data suara menjadi data vektor numerik agar dapat dilanjutkan ke tahap selanjutnya. Setelah data suara telah diubah ke dalam bentuk vektor numerik maka data vektor suara akan dilanjutkan ke tahap pra-pemrosesan untuk mengurangi noise pada data suara menggunakan teknik *Linear Predictive Coding* sehingga menghasilkan Koefisien Fitur Suara. Fitur suara yang telah berhasil diekstrak kemudian digunakan sebagai sumber data latih pada pembentukan model klasifikasi suara dengan teknik *Gaussian Mixture Models.*

Model Gaussian Mixture Models (GMM) yang dibuat akan memiliki jumlah komponen gaussian sesuai jumlah akun pengguna yang telah di registrasi, kemudian model GMM yang terbentuk digunakan untuk memberi label pada data suara pengguna yang telah dipetakan dengan akun pemilik suara sebelumnya. Berikut merupakan sampel pemetaan label data suara dengan akun pengguna. Ini ditunjukan pada Tabel 1.

Tabel 1 Sampel Pemetaan Akun Pengguna dan Detail Data Suara

Username	Data Suara	Label
User1	Data suara 1.wav	8
User1	Data suara 2.wav	7
User1	Data suara 3.wav	8
User1	Data suara 4.wav	8
User1	Data suara 5.wav	7

Proses Autentikasi suara pada sistem login dilakukan dengan membandingkan label data suara yang dimiliki oleh akun pengguna dengan label data suara yang diperoleh saat mengklasifikasikan input suara pada tahapan autentikasi suara, jika hasil perbandingan menunjukan label data suara input merupakan bagian dari label data suara yang dimiliki pemilik akun maka pengguna berhasil melakukan autentikasi suara dan berhasil login.

Dengan menggunakan metode di atas, model klasifikasi suara berhasil mendapatkan akurasi 67% dalam mengklasifikasikan data suara yang direkam langsung pada aplikasi, dan berhasil mendapatkan akurasi sebesar 75% dalam mengklasifikasikan data suara yang dikumpulkan dalam bentuk file dengan format WAV.

Setelah melakukan pengujian pada performa model GMM dalam mengklasifikasikan data suara, proses pengujian dilakukan pada sisi keamanan dari aplikasi yang dirancang. Beberapa pengujian keamanan yang dilakukan yaitu *Penetration Testing* untuk memindai celah keamanan pada sistem yang dirancang, *SQL Injection* untuk menguji kerentanan sistem terhadap injeksi kode yang mempengaruhi hasil yang diperoleh pada proses *backend* program, dan XSS *Attack* untuk menguji keamanan sistem terhadap injeksi kode yang biasanya bekerja pada browser. Hasil yang didapat dari serangkaian pengujian yang dilakukan adalah Sistem yang dirancang tidak rentan terhadap serangan *SQL Injection* ataupun *XSS Attack.*

4. KESIMPULAN

Penelitian yang dilakukan bertujuan untuk mengetahui efektivitas performa metode *Linear Predictive Coding* dan *Gaussian Mixture Models* dalam mengklasifikasikan data suara, dan cara meningkatkan keamanan sistem login suatu aplikasi dengan menerapkan autentikasi tambahan yaitu autentikasi biometrik suara. Pengumpulan data suara dilakukan dengan menggunakan *Google Form* dengan jumlah responden sebanyak 30 responden dan total jumlah data file suara sejumlah 150 file dengan format WAV, data suara yang dikumpulkan kemudian dibagi menjadi data latih dan data uji. Data suara yang telah dibagi menjadi data latih dan data uji kemudian diekstrak fitur – fitur nya dengan teknik LPC dan hasilnya digunakan sebagai sumber data pelatihan *Gaussian Mixture Models* dengan jumlah komponen sesuai dengan jumlah identitas pemilik suara, model yang terbentuk memberikan akurasi 67%, tingkat akurasi yang tergolong rendah disebabkan banyak faktor seperti kerentanan model klasifikasi suara terhadap noise, perbedaan kualitas perangkat yang digunakan sebagai media perekaman suara, dan kemiripan suara antara satu pengguna dengan pengguna lainnya. Hasil dari serangkaian pengujian pada aplikasi yang menerapkan autentikasi suara menunjukan bahwa autentikasi biometrik suara berhasil meningkatkan keamanan sistem login.

UCAPAN TERIMA KASIH

Terima kasih kepada bapak Novario Jaya Perdana, S.Kom., M.T yang telah memberikan saran untuk sehingga saya dapat menyelesaikan jurnal ini. Jurnal Computatio berterima kasih kepada IJCCS sebagai landasan bentuk format makalah ini.

DAFTAR PUSTAKA

[1] Carrasco, Oscar Contreras, 2019, "Gaussian Mixture Models Explained From intuition to implementation", *https://towardsdatascience.com/gaussian-mixture-models-explained-6986aaf5a95*, diakses tanggal 1 Januari 2022.

[2] Fachri, Fahmi, Abdul Fadlil, Imam Riadi, 2021, "Analisis Keamanan Webserver menggunakan Penetration Test", Jurnal Informatika Vol.8 No.2, hal. 183-190.

[3] Kenshanahan, Agaton, 2021, "Hati-hati, Ini 10 Jenis Serangan Siber yang Paling Sering Diadukan ke BSSN", *https://kumparan.com/kumparannews/hati-hati-ini-10-jenis-serangan-siber-yang-paling-sering-diadukan-ke-bssn-1vm9KCfDTGq/full*, diakses tanggal 1 Januari 2022.

[4] Singh, Aishwarya, 2019, "Build Better and Accurate Clusters with Gaussian Mixture Models", *https://www.analyticsvidhya.com/blog/2019/10/gaussian-mixture-models-clustering/*, diakses tanggal 31 Agustus 2021.

[5] S, Kristen, "Cross Site Scripting (XSS)", *https://owasp.org/www-community/attacks/xss/,* diakses tanggal 2 Januari 2022.

[6] W.S. Mada Sanjaya, Dyah Anggraeni, Ikhsan Purnama Santika, 2017, Speech Recognition using Linear Predictive Coding (LPC) and Adaptive Neuro-Fuzzy (ANFIS) to Control 5 DoF Arm Robot, Journal of Physics: Conference Series.