Computatio: Journal of Computer Science and Information Systems, 5/1 (2021), 1 – 6

ANALISIS SECURITY VOICE AUTHENTICATION PADA SISTEM LOGIN TWO FACTOR AUTHENTICATION

Gilbert Alexandro Onggo[1], Dyah Erny Herwindiati[2], Janson Hendryli[3]
Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Tarumanagara,
Jln. Letjen S. Parman No. 1, Jakarta, 11440, Indonesia
E-mail: [1]gilbert.535170006@stu.untar.ac.id, [2]dyahh@fti.untar.ac.id, [3]jansonh@fti.untar.ac.id

Abstrak

Program Sistem Login dengan API Otentikasi Suara merupakan sebuah program website yang dibuat untuk memberikan contoh untuk pengembang lain agar dapat membuat website sistem login yang aman. Program ini dibuat menggunakan bahasa pemrograman Python dengan program pengembangan Visual Studio Code, sedangkan berbagai modul dalam program menggunakan Flask dan MongoDB. Hasil dari pengujian program berupa analisa kerentanan program terhadap serangan injeksi SQL, XSS dan Replay. Hasil yang didapatkan berupa kerentanan terhadap penyerangan XSS dan terutama Replay. Serangan XSS dan injeksi dapat terjadi apabila program tidak ada proses filter terhadap bahasa pemrograman pada input. Serangan Replay dapat ditembus karena penggunaan token berbasis waktu. Penyerang dapat mengirim ulang data yang di rekam sebelum token kadaluwarsa. Untuk mencegah kebocoran data, program website dan API harus menggunakan Koneksi yang terenkripsi seperti SSL / TSL. API otentikasi suara dapat melakukan klasifikasi pengguna dengan akurasi 81.25% menggunakan 3 suara sebagai input awal. Namun, API otentikasi suara gagal dalam mencegah serangan replay spoofing dengan akurasi 66.66%. Kuesioner juga diberikan kepada pengembang lain mengenai contoh program yang dibuat dengan 32 responden. Hasil dari kuesioner menunjukkan bahwa "Analisis Security Voice Authenticator pada Sistem Login Two Factor Authentication" dapat menambah ilmu cybersecurity bagi pengembang lainnya.

Kata kunci*—Cyber Security, Voice Recognition, GMM, Python*

Abstract

The Login System Program with the Voice Authentication API is a website program designed to provide examples for other developers to create a secure login system website. This program was created using the Python programming language with the Visual Studio Code development program, while various modules in the program uses Flask and MongoDB. The results of program testing are in the form of program vulnerability analysis against SQL injection attacks, XSS and Replay. The results obtained are vulnerability to XSS attacks and especially Replay. XSS attacks and injection can occur if the program does not have a filter process against the input programming language. The replay attack is impenetrable due to the use of time-based tokens. The attacker can resend recorded data before the token expires. To prevent data leakage, website programs and APIs must use an encrypted connection such as SSL / TSL. Voice authentication API can perform user classification with 81.25% accuracy using 3 voices as initial input. However, the voice authentication API failed in preventing replay spoofing attacks with an accuracy of 66.66%. Questionnaires were also given to other developers regarding sample programs made with 32 respondents. The results of the questionnaire show that "Analysis of

Security Voice Authenticator on the Two Factor Authentication Login System" can add knowledge of cybersecurity for other developers.

Keywords— *Cyber Security, Voice Recognition, GMM, Python*

1. PENDAHULUAN

Pengenalan secara biometrik, menawarkan solusi yang andal untuk masalah otentikasi pengguna dalam sistem manajemen identitas [1]. Ada banyak alat dan teknik yang dapat mendukung pengelolaan keamanan informasi. Tetapi sistem berbasis biometrik telah berkembang untuk mendukung beberapa aspek keamanan informasi. Otentikasi biometrik mendukung aspek identifikasi, otentikasi, dan non-penolakan dalam keamanan informasi [2].

Menyusul ini, beberapa perusahaan besar telah mengambil sendiri untuk bertindak sebagai pelopor untuk otentikasi biometrik suara Namun, agar teknologi ini menjadi umum di semua industri, ada kebutuhan yang lebih besar akan solusi yang berhubung, andal, dan aman. Misalnya, teknologi ini harus mampu beradaptasi dengan fakta bahwa suara manusia berubah dari waktu ke waktu, harus bebas dari kebisingan latar belakang dan dapat mengidentifikasi pengguna dengan akurat. Untuk melakukan otentikasi biometrik, dibutuhkannya *Application Programming Interface* (API) yang akan digunakan pada sistem login yang digunakan sebagai penguhubung antar aplikasi UI dengan program backend.

Jurnal ini membahas mengenai kerentanan yang dapat dijumpai sistem login yang diintegrasikan dengan API voice authenticator menggunakan Aplikasi Web. Sistem Login dengan API voice authenticator merupakan tambahan keamanan login yang awalnya pengguna cukup melakukan otentikasi dengan password. Dengan API ini pengguna wajib menginput suara agar dapat dilakukan otentikasi pada program yang terhubung dengan API tersebut.

2. METODE PENELITIAN

Pengamatan dilakukan pada penyerangan sistem login bertujuan untuk menganalisis kerentanan koneksi antar sistem dengan penyedia layanan otentikasi biometrik suara sehingga dapat mencari cara untuk mencegah kerentanan tersebut. Pengguna akan diminta untuk memasukkan username dan password, jika user ditemukan pada database maka pengguna akan melanjutkan ke tahap berikutnya yaitu berupa input suara pengguna untuk dapat di verifikasi menggunakan API untuk dapat di verifikasi pada program backendnya. Hasil evaluasi dari sistem yang dibuat diukur dari ketangguhan terhadap gangguan dari serangan-serang yang dilakukan, seperti serangan Replay, Injection dan serangan XSS. Metode-metode tersebut merupakan metode yang sering digunakan oleh penyerang karena kemudahan akses atas alat dan kemudahan untuk dipelajari.

2.1 Preprocessing

Preprocessing dilakukan untuk mengolah data audio mentah menjadi data yang bisa proses oleh tahap selanjutnya. Untuk sistem ini Mel-Frequency Cepstral Coefficients dipilih karena merupakan fitur yang sering digunakan dalam analisa suara. MFCC di dasari pada cepstral coefficient dikomputasikan sebagai logaritma energi yang didaptkan dari filtrasi sinyal menggunakan filter triangular band-pass pada skala mel-frequency [3].

2.2 Gaussian Mixture Model

GMM merupakan model statistik dari distibusi probabilitas yang didapatkan dari nilai bobot setiap distribusi Gaussian sehingga GMM merupakan metode yang sangat tepat untuk perhitungan, baik dengan parameter maupun tidak. Bila model telah dihasilkan, syarat peluang dapat dihitung dan GMM juga dapat ditampilkan sebagai bentuk fungsi hubungan dasar network [4].

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

2.2.1 Expectation-Maximization (EM)

Expectation-Maximization adalah algoritma iterasi untuk melakukan estimasi kemungkinan maksimum, dan biasanya digunakan ketika ekspresi bentuk tertutup untuk memperbarui parameter model dapat dihitung. Algoritma ini terdiri dari dua langkah yaitu Expectation atau E-step dan Maximization M-step, fungsi E-step dapat dilihat sebagai berikut.

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

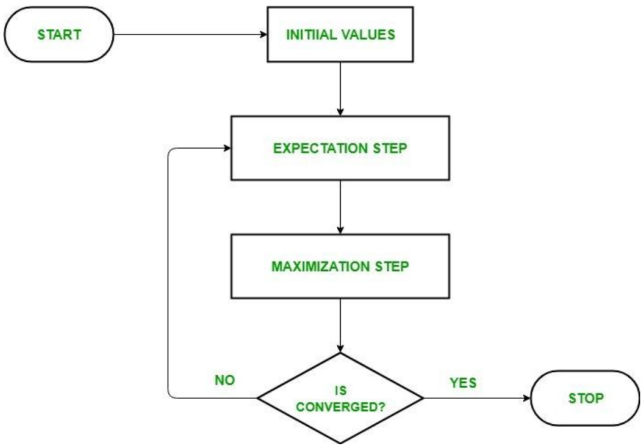
Kemudian untuk fungsi M-step dimana menghitung mean, probabilitas, dan kovarian dapat dilihat sebagai berikut.

$$\mu_j{}^{[k+1]} = \frac{\sum_i E[z_{i,j}|\mu^{[k]} \cdot x_i]}{\sum_i E[z_{i,j}|\mu^{[k]}]} \quad (3)$$

$$\pi_j{}^{[k+1]} = \frac{\sum_i E[z_{i,j}|\mu^{[k]}]}{N} \quad (4)$$

$$\Sigma_j{}^{[k+1]} = \frac{\sum_i E[z_{i,j}|\mu^{[k]}](x_i-\mu_j{}^{[k+1]})(x_i-\mu_j{}^{[k+1]})^T}{\sum_i E[z_{i,j}|\mu^{[k]}]} \quad (5)$$

Dengan tahapan diatas dapat di pahami bahwa alur GMM berupa inisialisasi, E-step, M-step kemudian kembali ke E-step lagi untuk melakukan iterasi sampai selesai. Diagram alur GMM dapat dilihat pada Gambar 1.



Gambar 1 Diagram Alur GMM (Sumber: https://www.codingninjas.com/blog/2020/09/15/what-is-em-algorithm-in-machine-learning/)

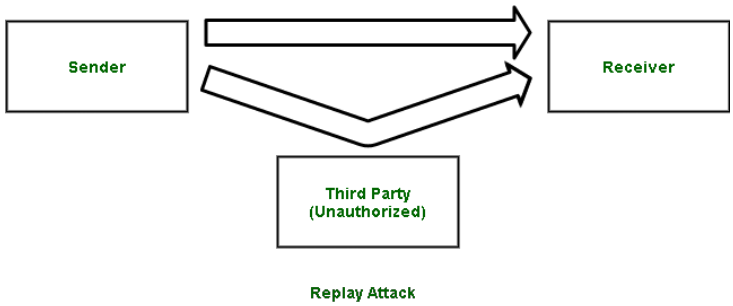
2.2.2 Clustering

Gaussian Mixture model sendirinya merupakan metode clustering. Sesuai dengan namanya Gaussian mixture model melibatkan campuran dari beberapa gaussian. Dibandingkan

mencari cluster berdasarkan sentroid "terdekat", model ini melakukan fitting sebuah set k gaussian ke data. Untuk perancangan ini akan dilakukan fitting ke gaussian dengan set ($12 \leq k \leq 20$) untuk dapat memilih banyak komponen yang terbaik untuk melakukan pengenalan suara pengguna.

2.3 Replay Attack

Serangan replay terjadi ketika penyerang menguping komunikasi jaringan yang aman, mencegatnya, dan kemudian secara curang menunda atau mengirimnya kembali untuk menyesatkan penerima agar melakukan apa yang diinginkan penyerang. Bahaya tambahan dari serangan replay adalah bahwa seorang penyerang bahkan tidak membutuhkan keterampilan tingkat lanjut untuk mendekripsi pesan setelah menangkapnya dari jaringan. Serangan itu bisa berhasil hanya dengan mengirim ulang semuanya [5].



Gambar 1 Arsitektur Serangan Replay (Sumber: https://www.geeksforgeeks.org/replay-attack/)

2.4 Injection Attack

Injection merupakan metode serangan dimana penyerang melakukan panggilan pada API yang memiliki SQL, NoSQL, LDAP, OS, atau perintah lain yang API atau program backend dibelakang-Nya menjalankan panggilan tersebut secara buta. Untuk melakukan serangan ini, penyerang harus menebak perintah apa yang dapat digunakan untuk API tersebut, bentuk panggilan, tipe data, dan banyak data.

2.5 XSS Attack

XSS attack merupakan sub kategori dari serangan injection yang lebih fokus ke access point sebuah website. Serangan XSS merupakan bentuk penyerangan cross site scripting dimana penyerang melakukan injeksi kode berbahaya secara langsung ke HTML aplikasi website. Serangan ini biasanya ditujukan ke pengguna lainnya yang tidak dapat mengetahui bahwa kode berbahaya di jalankan karena kode tersebut datang dari asal yang terpercaya. Kode berbahaya tersebut dapat mengambil cookies atau sesi dari pengguna tersebut dan dikirimkan ke penyerang apabila dijalankan.

3. HASIL DAN PEMBAHASAN

Eksperimen dilakukan dengan mengumpulkan suara manusia yang menyebut nama lengkapnya di halaman registrasi. Suara-suara tersebut direkam menggunakan mikrofon bawaan perangkat mereka dalam format WAV dari 13 subjek di mana setiap orang mengucapkan nama lengkap mereka tanpa kesamaan satu sama lain. Data dibagi menjadi pelatihan tanpa validasi dan pengujian yang ditetapkan untuk mensimulasikan otentikasi suara yang sebenarnya. Setiap dataset terdiri dari 3 speaker wanita dan 9 speaker pria dengan panjang dan bitrate yang sama. Set pelatihan hanya mencakup 3 suara dan 4 suara untuk pengujian.

Dengan menggunakan koefisien cepstral frekuensi-Mel, atau MFCC, sebagai representasi vektor suara. Fitur yang diekstrak kemudian dihitung deltanya dan digabungkan sebelum dipasang ke GMM. Saat ketiga suara dipasang ke GMM, GMM yang dipasang akan disimpan ke dalam penyimpanan lokal API untuk digunakan sebagai pengenalan. Saat API menerima perintah pengenalan untuk suara pengguna tertentu, API kemudian akan memeriksa setiap model GMM yang dibuat untuk menemukan model mana yang memiliki probabilitas terbaik untuk identifikasi pengguna. Jika model pengguna dan id pengguna cocok maka pengguna diautentikasi. Koneksi menggunakan TLS / SSL untuk mengenkripsi koneksi untuk server. Server login menggunakan token berbasis waktu untuk koneksinya ke API, kami membatasi waktu hingga 5 detik untuk setiap panggilan setelah mempertimbangkan waktu untuk mengunggah dan waktu perjalanan data dari satu server ke server lain untuk mensimulasikan API pihak ketiga.

Dengan menggunakan metode di atas, kami berhasil mendapatkan akurasi 81,16% dengan 14 komponen Gaussian dan 500 iterasi menggunakan suara pengujian pengguna. Ini ditunjukkan pada Tabel 1.

Tabel 1 Akurasi Pada Setiap Komponen

Banyak Komponen	Akurasi
12	75.0%
13	79.17%
14	81.25%
15	79.17%
16	62.5%
17	77.08%
18	66.67%
19	64.58%

Dengan hasil GMM yang cukup memuaskan kami melanjutkan melakukan pengetesan dengan metode serangan Replay, Injection, dan XSS. Hasil yang di dapatkan adalah sebagai berikut.

Tabel 1 Hasil Pengetesan Serangan

Jenis Serangan	**Kerentanan**	**Keberhasilan**
Replay	Besar	Berhasil
Injection	-	Gagal
XSS	Rendah	Berhasil

Serangan pada replay dan XSS berhasil sedangkan serangan injection gagal. Hal ini dikarenakan beberapa hal, yaitu Python dapat mengunci object string input agar tidak dapat dikategorikan sebagai Bahasa pemrograman sehingga tetap dianggap sebagai string dan SQLAlchemy yang digunakan pada sistem API untuk mengendalikan database user memiliki pertahanan sendiri terahadap serangan SQL selama kode system tidak menggunakan Bahasa SQL mentah. Serangan XSS dapat di cegah dengan menggunakan autoescape yang dimana dapat dinyalakan pada setiap input user, karena itu kerentanan untuk serangan ini dianggap rendah. Sedangkan serangan replay sangat tinggi, karena apabila penyerang berhasil menangkap paket data yang dikirimkan oleh user, penyerang dapat menembus otentikasi sistem. Salah satu cara lain oleh penyerang yaitu dengan melakukan perekaman suara ke user kemudian mengirim hasil rekaman tersebut ke server, maka hasil yang sama dapat terjadi. Hasil akurasi penyerangan replay dengan cara ini memberikan 66.67% keberhasilan oleh penyerang melakukan otentikasi tidak sah.

4. KESIMPULAN

Penelitian ini mengeksplorasi sistem otentikasi berbasis suara pada sistem login menggunakan GMM. Kami menguji kerentanan keamanan terhadap penggunaan replay, injeksi, dan serangan XSS untuk menemukan kelemahan yang ditemukan dalam sistem tersebut. Pengumpulan data suara dari 13 subjek menghasilkan 48 rekaman yang kemudian dipecah menjadi training tanpa validasi, dan test set. Model GMM terbaik dilatih menggunakan 14 komponen dan 1000 iterasi, memberikan akurasi 81,16%. Meskipun demikian, model tersebut masih menerima percobaan login ilegal (false positive) dengan tingkat 66.67% dan membutuhkan eksplorasi yang lebih mendalam untuk menemukan cara yang dapat diandalkan untuk melawan jenis serangan ini. Fakta lain yang memprihatinkan adalah jika seseorang memiliki suara yang mirip dengan pengguna, dia dapat diautentikasi secara salah dan dapat melihat data pengguna bahkan tanpa mencoba serangan yang diuji.

UCAPAN TERIMA KASIH

Terima kasih kepada Janson Hendryli S. Kom., M. Kom 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] Anil K. Jain, Karthik Nandakumar, Abhishek Nagar, 2008, Biometric template security, EURASIP Journal on Advances in Signal Processing.

[2] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A., dan Minkyu Choi., 2009, Biometric Authentication: A Review, *International Journal of u- and e- Service, Science and Technology* Vol. 2, No. 3.

[3] S. B. Davis and P. Mermelstein, 1980, Comparison of parametric representation for monosyllabic word recognition in continuously spoken sentences, *IEEE Transactions on Acoustics, Speech and Signal Processing,* vol. 28, no. 4, hal. 357–366.

[4] Palaanen, Joni-Kristian Kamarainen, Jarmo Ilonen, Heikki Kälviäinen, 2006. Feature representation and discrimination based on Gaussian mixture model probability densities Practices and algorithms, *Pattern Recognition*, Vol. 39, No. 7, hal. 1346-1358

[5] Marcin Witkowski, Stanisław Kacprzak, Piotr Zelasko, Konrad Kowalczyk, Jakub Gałka, 2017, Audio Replay Attack Detection Using High-Frequency Features, *Interspeech*