

BAB 5. PENUTUP

Bab ini berisi kesimpulan dan saran berdasarkan hasil penelitian yang telah dilakukan. Kesimpulan disusun untuk menjawab rumusan masalah dan tujuan penelitian terkait rancang bangun aplikasi DokuSafe sebagai aplikasi penyimpanan dokumen pribadi berbasis Android dengan autentikasi *voice biometric* menggunakan ECAPA-TDNN. Sementara itu, saran diberikan sebagai masukan untuk pengembangan sistem pada penelitian selanjutnya, khususnya pada aspek peningkatan keamanan, performa, dan pengembangan fitur aplikasi.

5.1. Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, dapat disimpulkan sebagai berikut:

1. Penelitian ini berhasil merancang dan membangun aplikasi DokuSafe sebagai aplikasi penyimpanan dokumen pribadi berbasis Android yang menerapkan autentikasi biometrik suara menggunakan model ECAPA-TDNN. Pengembangan sistem dilakukan dengan metode *Rapid Application Development* (RAD), mulai dari tahap analisis kebutuhan, perancangan sistem, implementasi, hingga pengujian. Aplikasi berhasil mengintegrasikan beberapa komponen utama, yaitu autentikasi akun menggunakan email dan *password*, autentikasi biometrik suara berbasis ECAPA-TDNN, deteksi *anti-spoofing* menggunakan model Nes2Net-X, serta mekanisme pengamanan dokumen menggunakan algoritma AES-256 dengan Android Keystore. Selain itu, metadata dokumen dikelola menggunakan *Room Database* sehingga proses penyimpanan, pencarian, dan pengelolaan dokumen dapat dilakukan secara efisien. Integrasi seluruh komponen tersebut menghasilkan aplikasi yang mengimplementasikan mekanisme autentikasi berlapis dan pengamanan dokumen sebagai upaya untuk membatasi akses terhadap dokumen pada perangkat Android.
2. Penelitian ini berhasil mengevaluasi kinerja sistem verifikasi biometrik suara berbasis ECAPA-TDNN yang diimplementasikan pada aplikasi DokuSafe dari aspek kecepatan proses, efisiensi penggunaan sumber daya, dan stabilitas sistem pada perangkat *mobile*. Hasil *Performance Testing* menunjukkan bahwa proses *Login*, *enrollment* suara, verifikasi suara, unggah dan enkripsi dokumen, serta pembukaan dokumen terenkripsi memiliki waktu respons yang layak untuk mendukung penggunaan aplikasi secara interaktif. Pengukuran menggunakan Android Profiler juga menunjukkan bahwa penggunaan CPU dan memori selama proses

otentikasi maupun pengelolaan dokumen masih berada pada tingkat yang wajar, sehingga aplikasi dapat dijalankan tanpa memberikan beban sumber daya yang berlebihan pada perangkat. Selain itu, hasil *Unit Testing*, *Integration Testing*, dan *System Testing* menunjukkan bahwa seluruh modul dan integrasi sistem berjalan sesuai dengan kebutuhan fungsional tanpa ditemukan kegagalan selama proses pengujian. Penerapan mekanisme *envelope encryption* juga terbukti mampu meningkatkan performa proses pembukaan dokumen terenkripsi secara signifikan dibandingkan implementasi sebelumnya. Evaluasi pipeline autentikasi end-to-end pada berbagai kondisi penggunaan juga menunjukkan bahwa sistem mampu memberikan keputusan autentikasi yang sesuai pada sebagian besar skenario pengujian, meskipun masih ditemukan beberapa kasus *false rejection* pada kondisi tertentu dan *false acceptance* pada skenario *playback attack* tertentu. Secara keseluruhan, hasil penelitian menunjukkan bahwa aplikasi DokuSafe berhasil mengintegrasikan autentikasi biometrik suara berbasis ECAPA-TDNN, deteksi *anti-spoofing* menggunakan Nes2Net-X, serta mekanisme pengamanan dokumen pada platform Android. Hasil pengujian menunjukkan bahwa seluruh komponen tersebut telah berfungsi sesuai dengan kebutuhan fungsional dan memberikan hasil yang sesuai pada sebagian besar skenario pengujian yang dilakukan.

5.2. Saran

Berdasarkan hasil penelitian yang telah dilakukan, aplikasi DokuSafe masih memiliki beberapa aspek yang dapat dikembangkan lebih lanjut agar sistem menjadi lebih optimal, aman, dan siap digunakan dalam kondisi nyata. Adapun beberapa saran yang dapat dijadikan pertimbangan untuk penelitian atau pengembangan selanjutnya adalah sebagai berikut:

1. Penelitian selanjutnya dapat mengembangkan sistem autentikasi biometrik suara agar dapat berjalan secara penuh pada perangkat Android atau *full offline*. Pengembangan ini dapat dilakukan dengan mengoptimalkan model verifikasi pembicara ECAPA-TDNN dan model *anti-spoofing* Nes2Net-X agar dapat diimplementasikan secara *on-device*, misalnya melalui proses konversi model ke format yang lebih ringan dan sesuai untuk perangkat *mobile*. Dengan demikian, proses pendaftaran suara dan verifikasi suara dapat dilakukan secara *real-time* tanpa bergantung pada koneksi jaringan pengguna maupun ketersediaan *backend* server.

2. Sistem penyimpanan *speaker embedding* pada *backend* masih dapat dikembangkan lebih lanjut agar lebih aman. Pada penelitian ini, *speaker embedding* pengguna disimpan dalam bentuk *file .npz* karena format tersebut sederhana dan sesuai untuk kebutuhan prototipe. Namun, untuk pengembangan pada lingkungan produksi, penyimpanan *embedding* sebaiknya tidak hanya mengandalkan *file .npz*, melainkan diintegrasikan dengan modul keamanan khusus untuk data biometrik. Modul tersebut dapat mencakup enkripsi *embedding*, pengelolaan kunci yang aman, kontrol akses, validasi integritas, serta pencatatan aktivitas akses terhadap data *embedding*. Dengan demikian, *embedding* suara pengguna dapat terlindungi dari risiko akses tidak sah, penyalinan, modifikasi, maupun penyalahgunaan oleh pihak yang tidak berwenang.
3. Penelitian selanjutnya disarankan menggunakan *dataset* suara dengan jumlah partisipan yang lebih banyak dan karakteristik yang lebih beragam, seperti variasi usia, jenis kelamin, aksen, perangkat perekaman, serta kondisi lingkungan yang berbeda. Penggunaan *dataset* yang lebih besar dan representatif diharapkan mampu memberikan evaluasi yang lebih komprehensif terhadap performa sistem, sekaligus meningkatkan kemampuan generalisasi model verifikasi biometrik suara sehingga lebih adaptif terhadap berbagai kondisi penggunaan di dunia nyata.
4. Pengembangan aplikasi dapat diarahkan pada peningkatan fitur keamanan tambahan, seperti penerapan *backup* terenkripsi, sinkronisasi *cloud* yang aman, mekanisme pemulihan akun, serta autentikasi multifaktor. Fitur-fitur tersebut dapat membantu meningkatkan keandalan aplikasi sebagai penyimpanan dokumen pribadi, terutama apabila pengguna mengganti perangkat atau kehilangan akses ke perangkat lama. Namun, pengembangan fitur tersebut tetap perlu memperhatikan prinsip keamanan data agar dokumen pribadi pengguna tidak tersimpan atau berpindah tanpa perlindungan enkripsi yang memadai.
5. Dari sisi *backend*, sistem penyimpanan *embedding* suara dapat dikembangkan menggunakan mekanisme penyimpanan yang lebih terstruktur dan aman, misalnya dengan *database* khusus atau object storage yang dilengkapi kontrol akses. Selain itu, komunikasi antara aplikasi Android dan *backend* perlu diamankan secara penuh menggunakan HTTPS ketika sistem diterapkan pada lingkungan produksi. Hal ini penting agar data audio, hasil verifikasi, serta informasi autentikasi pengguna tidak rentan terhadap penyadapan selama proses pertukaran data antara *client* dan server.

Dengan adanya pengembangan lebih lanjut pada aspek *dataset*, pengujian, keamanan, performa, dan infrastruktur *backend*, aplikasi DokuSafe diharapkan dapat menjadi sistem penyimpanan dokumen pribadi yang lebih aman, stabil, dan siap digunakan dalam skenario penggunaan nyata.