

PERANCANGAN APLIKASI BIOGUARD OS UNTUK MENDUKUNG KEAMANAN SIBER YANG BERBASIS BIOMETRIK

Rakhmadi Rahman¹, Annisa Arthanty², Muhammad Adhi Fahriansyah Ahmad³

^{1,2,3} Sistem Informasi, Jurusan Sains, Institut Teknologi Bacharuddin Jusuf Habibie

Email : ¹rakhmadi.rahman@ith.ac.id ²annisaarthanty21@gmail.com,

³adhyfahriansyah123@gmail.com

Diterima : 30 Juni 2024 ; Disetujui : 16 Juli 2024 ; Dipublikasikan : 31 Juli 2024

ABSTRAK

Dalam era digital yang semakin terhubung, keamanan siber menjadi aspek yang sangat penting bagi sistem operasi. Ancaman terhadap keamanan data semakin canggih, sehingga menuntut pengembangan solusi autentikasi yang lebih kuat. Salah satu solusi yang diusulkan adalah integrasi teknologi biometrik ke dalam sistem operasi, seperti yang dilakukan dalam *BioGuard OS*. Perancangan ini bertujuan untuk mengevaluasi efektivitas *BioGuard OS* dalam melindungi sistem dari ancaman siber dengan menggunakan teknologi biometrik. Biometrik berasal dari kata Yunani "*bios*" yang berarti hidup dan "*metron*" yang berarti ukuran, dan secara ilmiah, biometrik adalah teknologi yang berfokus pada pengenalan makhluk hidup berdasarkan karakteristik unik masing-masing individu. Teknologi biometrik didefinisikan sebagai penggunaan otomatis karakteristik fisiologis atau perilaku untuk menentukan atau memverifikasi identitas seseorang. Teknologi ini mencoba menghasilkan model komputer dari karakteristik fisik dan perilaku manusia dengan tujuan identifikasi pribadi yang dapat diandalkan. Dalam *BioGuard OS*, teknologi biometrik yang digunakan untuk meningkatkan keamanan siber termasuk pengenalan wajah, sidik jari, dan pengenalan suara. Analisis informasi biometrik telah menjadi perhatian sejak lama, dengan berbagai solusi autentikasi berdasarkan karakteristik seperti tanda tangan, sidik jari, integrasi wajah, geometri tangan, serta pemindaian iris dan retina. Penelitian ini berfokus pada seberapa efektif *BioGuard OS* dalam menggunakan teknologi tersebut untuk melindungi sistem dari berbagai ancaman siber.

Kata Kunci : *BioGuard OS*, keamanan siber, sistem operasi, teknologi biometrik.

ABSTRACT

In our increasingly connected digital world, cybersecurity has become a crucial aspect of operating systems. As data security threats grow more sophisticated, the need for advanced authentication solutions intensifies. One proposed solution is the incorporation of biometric technology into operating systems, as demonstrated by BioGuard OS. This design aims to assess the effectiveness of BioGuard OS in safeguarding systems from cyber threats through biometric technology. Biometrics, derived from the Greek words "bios" (life) and "metron" (measure), scientifically refers to identifying individuals based on their unique characteristics. Biometric technology is defined as the automated use of physiological or behavioral traits to verify a person's identity. It attempts to create computer models of human physical attributes and behaviors for reliable personal identification. BioGuard OS employs biometric technologies such as facial recognition, fingerprint scanning, and voice recognition to enhance cybersecurity. The analysis of biometric information has long been a concern, with various authentication solutions leveraging characteristics like signatures, fingerprints, facial features, hand geometry, and iris and retina scanning. This research investigates how effective BioGuard OS is in utilizing these technologies to protect systems from diverse cyber threats..

Keywords : *BioGuard OS, biometric technology, cyber security, operating system.*

1. PENDAHULUAN

Dalam era digital yang semakin terhubung, keamanan siber menjadi aspek yang sangat penting bagi sistem operasi. Ancaman terhadap keamanan data semakin canggih, yang menuntut pengembangan solusi autentikasi yang lebih kuat. Salah satu solusi yang diusulkan adalah mengintegrasikan teknologi biometrik ke dalam sistem operasi, seperti yang dilakukan dalam *BioGuard OS*. Penelitian ini bertujuan untuk mengevaluasi sejauh mana *BioGuard OS* efektif dalam melindungi sistem dari ancaman siber dengan menggunakan teknologi biometrik.

Biometrik berasal dari bahasa Yunani, dengan kata "*bios*" yang berarti hidup dan "*metron*" yang berarti ukuran. Secara ilmiah, biometrik adalah teknologi yang berfokus pada pengenalan makhluk hidup berdasarkan karakteristik unik masing-masing individu [1].

Sedangkan teknologi biometrik didefinisikan sebagai penggunaan otomatis karakteristik fisiologis atau perilaku untuk menentukan atau memverifikasi identitas seseorang.

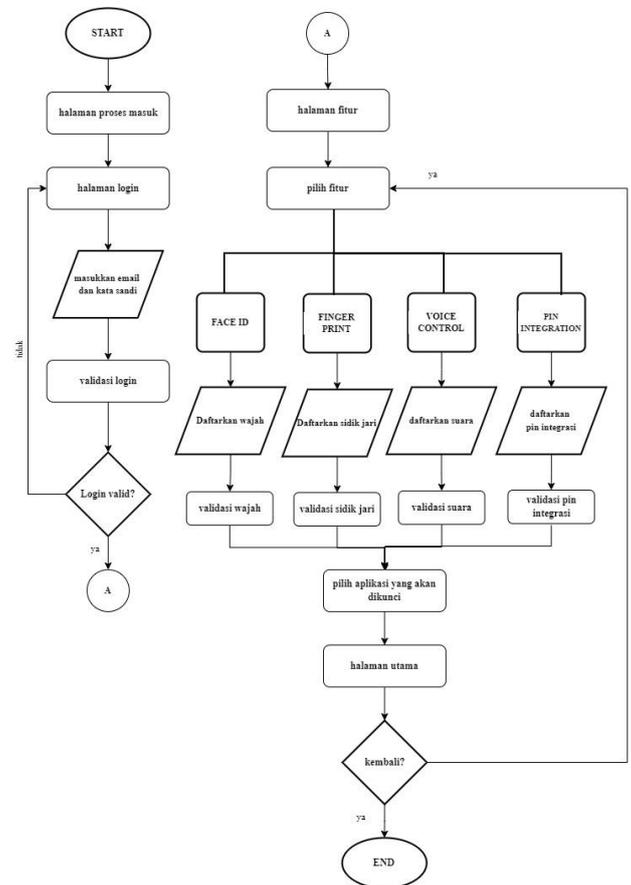
Teknologi ini mencoba menghasilkan model komputer dari karakteristik fisik dan perilaku manusia dengan tujuan identifikasi pribadi yang dapat diandalkan. Karakteristik ini mencakup gambar visual dan fenomena manusia lainnya seperti berbicara, berjalan, bau, DNA, dan fakta-fakta lain yang dapat membantu mengidentifikasi individu secara unik [2].

Analisis informasi biometrik telah menjadi perhatian sejak lama. Banyak peneliti telah mengembangkan solusi efisien untuk autentikasi manusia berdasarkan berbagai karakteristik seperti tanda tangan, sidik jari, wajah, geometri tangan, analisis penekanan tombol, telinga, gaya berjalan, serta pemindaian iris dan retina [3].

Penggunaan teknologi biometrik dalam *BioGuard OS* yang diambil untuk meningkatkan keamanan siber termasuk pengenalan wajah, sidik jari, dan pengenalan suara.

2. METODE

Penelitian ini menggunakan beberapa metode biometrik untuk meningkatkan keamanan siber pada *BioGuard OS*, termasuk pengenalan wajah, sidik jari, pengenalan suara, dan integrasi PIN.



Gambar 1. Flowchart Rancangan Aplikasi *BioGuard OS*

Gambar 1 menggambarkan alur proses aplikasi mulai dari halaman login hingga validasi biometrik dan pemilihan fitur aplikasi yang akan dikunci. Pengguna memasukkan email dan kata sandi untuk validasi login, kemudian memilih fitur biometrik yang diinginkan, seperti Face ID, Fingerprint, Voice Control, atau PIN Integration. Setiap metode biometrik memiliki proses pendaftaran dan validasi tersendiri sebelum pengguna dapat memilih aplikasi yang akan dikunci. Alur ini juga memastikan bahwa setiap langkah keamanan dilakukan secara berurutan dan terverifikasi dengan baik, meningkatkan efektivitas sistem dalam melindungi data dan mencegah akses tidak sah.

3. HASIL DAN PEMBAHASAN

"BioGuard OS" terinspirasi oleh gabungan kata "Bio" yang merujuk pada biometrik, dan "Guard" yang berarti pengaman atau perlindungan. Penggunaan kata "OS" sendiri sebagai singkatan dari "Operating System" yang menegaskan bahwa *BioGuard OS* adalah sebuah sistem operasi. Jadi, nama tersebut mencerminkan fokus utama sistem operasi tersebut, yaitu menggabungkan teknologi biometrik dengan lapisan keamanan yang kuat untuk memberikan perlindungan yang tinggi terhadap data dan sistem.

Langkah-langkah yang dilakukan dalam merancang *BioGuard OS* sebagai berikut :

- BioGuard Os* dirancang dengan menggunakan figma.
- Kemudian berikut merupakan rancangan dari *BioGuard OS* :

Halaman Saat Proses Masuk

Pada halaman saat proses masuk akan menampilkan nama logo dan aplikasi



Gambar 2. Halaman on boarding BioGuard OS

Menu Pendaftaran dan Login

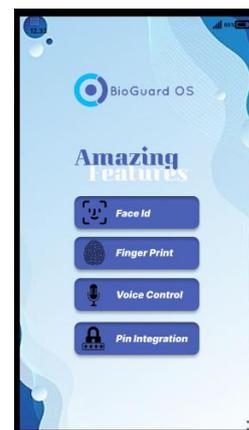
Pada halaman ini, tersedia opsi *login*, *create account* (mendaftar akun baru bagi pengguna yang belum memiliki akun), dan lanjutkan dengan google. Untuk mengakses aplikasi, pengguna perlu memasukkan *username* berupa email serta *password*, atau mereka bisa masuk lewat Google. Jika ingin membuat akun baru, pengguna harus mengisi formulir pendaftaran dengan nama lengkap, email, nomor handphone dan *password*, atau bisa juga mendaftar menggunakan akun Facebook atau Google.



Gambar 3. Menu Pendaftaran dan Login BioGuard OS

Menu Fitur

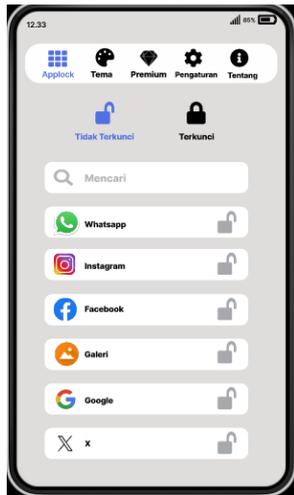
Di halaman ini, pengguna diberikan opsi untuk memilih sistem keamanan biometrik mana yang ingin digunakan. Terdapat empat pilihan sistem keamanan biometrik, termasuk identifikasi wajah (*Face ID*) di mana pengguna dapat mendaftarkan ciri wajah mereka, sidik jari (*Fingerprint*) di mana pengguna dapat mendaftarkan sidik jari mereka, kontrol suara (*Voice Control*) di mana pengguna dapat mendaftarkan suara mereka, dan integrasi PIN (*PIN Integration*) di mana pengguna dapat mendaftarkan nomor PIN yang akan digunakan.



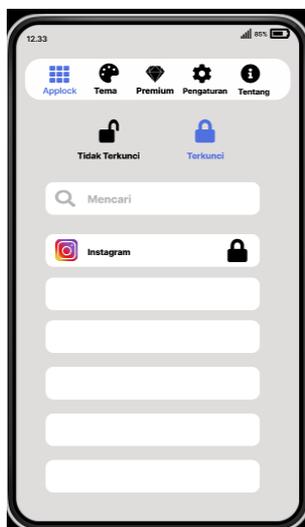
Gambar 4. Menu Fitur BioGuard OS

Menu Utama

Di halaman ini, tersedia dua pilihan: terkunci dan tidak terkunci. Pengguna dapat memilih aplikasi mana yang akan dikunci menggunakan sistem biometrik yang telah dipilih sebelumnya pada halaman fitur.



Gambar 5. Menu Home Tidak Terkunci BioGuard OS



Gambar 6. Menu Home Terkunci BioGuard OS

Halaman Scan Sidik Jari

Pada halaman ini berikut adalah tampilan *scan* sidik jari sebelum dan sesudah *di-scan*.



Gambar 7. Halaman Scan sidik jari sebelum di-scan



Gambar 8. Halaman Scan sidik Jari setelah di-scan

Tabel 1. Hasil Percobaan Pada User

Nama user	Face id	Sidik jari	Voice control	Pin Integration
caca	✓	✓	✓	✓
Adhy	✓	✓	x	✓
irfandy	✓	✓	x	✓
Shila	x	✓	✓	✓
sukma	✓	✓	✓	✓

Pada tabel 1 dapat dilihat hasil percobaan dari beberapa user. Dimana dari percobaan tersebut peneliti masih harus melakukan perkembangan agar semua percobaan pada keamanan biometriknya berhasil.

4. PENUTUP

4.1. Kesimpulan

keamanan siber menjadi aspek yang sangat penting bagi sistem operasi. Penelitian ini menyoroti pentingnya penggunaan teknologi biometrik untuk meningkatkan keamanan siber pada sistem operasi, seperti yang diterapkan dalam BioGuard OS. Dengan integrasi teknologi biometrik seperti pengenalan wajah, sidik jari, dan pengenalan suara, BioGuard OS menunjukkan potensi yang signifikan dalam melindungi sistem dari berbagai ancaman siber. Penggunaan karakteristik unik individu sebagai metode autentikasi menawarkan solusi yang lebih andal dan sulit untuk diretas dibandingkan dengan metode tradisional seperti kata sandi. Selain itu, alur proses aplikasi yang didesain secara berurutan dan terverifikasi meningkatkan keamanan dan efektivitas sistem dalam mencegah akses tidak sah.

4.2. Saran

Dalam meningkatkan efektivitas BioGuard OS, lakukan pengujian dan pembaruan sistem secara berkala. Tambahkan

fitur keamanan baru dan tingkatkan algoritma biometrik. Berikan pelatihan kepada pengguna tentang keamanan siber dan penggunaan teknologi biometrik. Kombinasikan teknologi biometrik dengan metode keamanan lain, seperti enkripsi data dan firewall, untuk perlindungan yang lebih kuat. Lakukan penelitian lanjutan untuk mengevaluasi sistem dalam berbagai kondisi penggunaan

5. DAFTAR PUSTAKA

- [1] Andarinny, A. A., Widodo, C. E., & Adi, K. (2017). Perancangan sistem identifikasi biometrik jari tangan menggunakan Laplacian of Gaussian dan ekstraksi kontur. In *Youngster Physics Journal* (Vol. 6, Issue 4).
- [2] Shen, P., Wang, P., Yanushkevich, S., Wang, P. S. P., & Yanushkevich, S. N. (2007). *Biometric technologies and applications*. <https://www.researchgate.net/publication/221173670>
- [3] Fakultas, J. E., & Oleh, T. (2017). *Disusun Sebagai Salah Satu Syarat Menyelesaikan Program Studi Strata I*.