Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 1 (2026) pp: 15109-15117
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Implementasi Teknologi *Biometric Authentication* Dalam Meningkatkan Keamanan Nasabah Pengguna *Mobile Banking*

[1]Dinda Ratu, [2]Hesi Eka Puteri
[12]Fakultas Ekonomi dan Bisnis Islam, UIN Sjech M. Djamil Djambek Bukittinggi
[1]dindaratu0505@gmail.com, [2]hesiekaputeri@gmail.com

Abstrak

Penelitian ini mengkaji penerapan otentikasi biometrik dalam meningkatkan keamanan mobile banking dengan studi kasus di BSI KC Bukittinggi Sudirman. Latar belakang penelitian didasarkan pada meningkatnya ancaman penipuan digital, seperti pembajakan akun, skimming, dan phishing, yang sering berkaitan dengan kebocoran data. Berdasarkan data OJK tahun 2023, tercatat 16.359 kasus penipuan pada layanan keuangan, sehingga metode keamanan tradisional seperti PIN dan kata sandi dinilai semakin rentan. Oleh karena itu, diperlukan sistem keamanan yang lebih kuat, salah satunya melalui penerapan otentikasi biometrik. Tujuan penelitian ini adalah menganalisis implementasi biometrik dalam menjaga keamanan transaksi, mengidentifikasi tantangan yang dihadapi, serta mengevaluasi dampaknya terhadap keamanan dan kepercayaan pengguna. Penelitian menggunakan metode deskriptif kualitatif dengan teknik pengumpulan data melalui wawancara mendalam. Analisis data dilakukan menggunakan model Miles dan Huberman yang meliputi reduksi data, penyajian data, dan penarikan kesimpulan. Hasil penelitian menunjukkan bahwa otentikasi biometrik telah diterapkan sebagai sistem keamanan berlapis, khususnya pada proses registrasi awal dan login aplikasi. Sementara itu, PIN dan kata sandi masih digunakan untuk otorisasi transaksi akhir. Pengguna menilai biometrik, seperti sidik jari dan pengenalan wajah, mampu meningkatkan keamanan sekaligus memberikan kemudahan dalam penggunaan. Namun, penerapan biometrik juga menghadapi beberapa kendala, baik internal maupun eksternal. Kendala internal meliputi keterbatasan fungsi biometrik dalam transaksi, sedangkan kendala eksternal mencakup kondisi perangkat dan jaringan pengguna. Secara keseluruhan, otentikasi biometrik terbukti meningkatkan keamanan dan kepercayaan pengguna, meskipun masih memerlukan kombinasi dengan metode keamanan lain.

***Kata kunci**: Keamanan Mobile Banking, Penipuan Digital, Kepercayaan Pengguna, Bank Syariah Indonesia*

1. Pendahuluan

Perkembangan digitalisasi di sektor finansial telah mengubah paradigma layanan keuangan perbankan. Data dari Otoritas Jasa Keuangan (OJK) menunjukkan bahwa permasalahan yang banyak ditanyakan, dilaporkan, atau diadukan pada sektor perbankan salah satunya adalah penipuan yang meliputi pembobolan rekening, *skimming, phising* ataupun kasus kebocoran data nasabah berjumlah 16.359 kasus.

Tabel 1.1
Jenis Permasalahan yang paling banyak dilaporkan

No	Jenis Pengaduan (Complaint Type)	Jumlah
1	Sistem Layanan Informasi Keuangan (SLIK)	33.451
2	Penipuan (Pembobolan rekening,skimming, phising, social engineering)	16.359
3	Perilaku Petugas Penagihan	6.214
4	Restrukturisasi Kredit Pinjaman	3.502
5	Penolakan Pelunasan Kredit Dipercepat	1.364

Sumber: Laporan Kinerja OJK Tahun 2023

Berdasarkan tabel 1.1 bahwa penipuan seperti pembobolan rekening, *skimming*, *phising*, *social engineering*, yang akar dari masalahnya adalah kebocoran data. Maka satu solusi yang menjanjikan untuk mengatasi dan mencegah masalah ini terus terjadi bahkan meningkat adalah penerapan teknologi *biometric authentication*. Teknologi ini merupakan sistem yang membaca bagian tubuh manusia untuk mengenali keaslian (*authentication*) yang unik dan tetap dari tubuh manusia seperti sidik jari, selaput pelangi mata/ iris maupun wajah yang disimpan dalam database teknologi *biometric.*

Teknologi ini telah menjadi komponen krusial dalam sistem keamanan modern karena kemampuannya yang mengidentifikasi individu berdasarkan karakteristik unik yang sulit dipalsukan, namun agar data *biometric* dapat dimanfaatkan secara luas dan aman, diperlukan perlindungan melalui teknik seperti *watermarking* dan enkripsi. Peningkatan ini tidak hanya memperkuat sistem dari sisi teknis, tetapi juga mendorong kepercayaan pengguna terhadap teknologi biometric.

Secara umum proses perbankan yang telah menerapkan teknologi *Biometric Authentication* adalah pada aplikasi *mobile banking*. Aplikasi ini memungkinkan pengguna untuk melakukan berbagai transaksi keuangan melalui ponsel, seperti transfer dana, pembayaran tagihan, dan manajemen rekening, langsung dari perangkat *mobile* mereka. Kemudahan akses yang ditawarkan oleh aplikasi *mobile banking* ini telah menjadikannya sangat marak di kalangan pengguna khususnya kalangan gen z yang sekarang lebih banyak bertransaksi dengan *cashless*. Fitur yang disediakan oleh *mobile banking*, yaitu *mobile banking* BSI seperti transfer sesama bank maupun antar bank, *top-up e-wallet, ziswaf*, waktu sholat, dan arah kiblat

Transaksi yang dilakukan pada *mobile banking* di Indonesia sejak 2 tahun terakhir mengalami peningkatan pada periode juni 2023-2024 terlihat pada tabel 1.2 berikut:

Tabel 1.2

Transaksi BSI Mobile Banking

No	Keterangan	Juni 2023	Juni 2024	Pertumbuhan (yoy)
1	Jumlah Pengguna BSI Mobile	3,26 Juta	7,1 Juta	
2	Jumlah Transaksi	170,7 Juta	247,5 Juta	
3	Volume Transaksi	220,5 triliun	299 triliun	
4	*Fee based income* (Jan-Jun)		178,2 miliar	37,09%
5	Pertumbuhan transaksi			45,02%

Sumber : Bank Syariah Indonesia (2024)

Berdasarkan tabel 1.2 terlihat bahwa layanan dari *mobile banking* mengalami pertumbuhan pengguna, transaksi, dan volume yang sangat pesat. Tidak menutup kemungkinan bahwa adanya peningkatan transaksi pada perbankan dan orang yang menggunakan *mobile banking* maka semakin besar pula potensi terjadinya kejahatan *cyber*. Maka dari itu keamanan transaksi menjadi perhatian utama dalam implementasi teknologi *biometric* ini. Data keuangan dan informasi pribadi nasabah merupakan sasaran yang sangat menarik bagi pelaku kejahatan *cyber*. Ancaman seperti pencurian identitas, penipuan, dan serangan siber semakin canggih dan dapat menimbulkan dampak serius pada nasabah serta reputasi bank.

Dalam konteks ini, teknologi *biometric* telah muncul sebagai salah salah satu Solusi yang menjanjikan dalam menghadapi tantangan keamanan dalam transaksi perbankan syariah. Seperti pada penjelasan sebelum- sebelumnya bahwa, *Biometric* mengacu pada metode identifikasi berdasarkan karakteristik fisik unik seseorang, seperti sidik jari, retina, atau pemindaian wajah. Ini adalah pendekatan yang jauh lebih aman daripada hanya menggunakan metode otentikasi tradisional, seperti kata sandi atau PIN, yang dapat dengan mudah diretas atau disalah gunakan.

Secara umum proses perbankan yang telah menerapkan teknologi *Biometric Authentication* adalah pada aplikasi *mobile banking*. Aplikasi ini memungkinkan pengguna untuk melakukan berbagai transaksi keuangan melalui ponsel, seperti transfer dana, pembayaran tagihan, dan manajemen rekening, langsung dari perangkat *mobile* mereka. Kemudahan akses yang ditawarkan oleh aplikasi *mobile banking* ini telah menjadikannya sangat marak di kalangan pengguna khususnya kalangan gen z yang sekarang lebih banyak

DOI: https://doi.org/10.31004/riggs.v5i1.8230
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

bertransaksi dengan *cashless*. Fitur yang disediakan oleh *mobile banking*, yaitu *mobile banking* BSI seperti transfer sesama bank maupun antar bank, *top-up e-wallet*, *ziswaf*, waktu sholat, dan arah kiblat (Bank Syariah Indonesia 2024).

Teori Temoshok pada NIST SP 800-63B memberikan landasan yang kuat bahwa implementasi teknologi *biometric authentication* dalam layanan *mobile banking* berkontribusi dalam meningkatkan keamanan nasabah, bukan sebagai pengganti sistem keamanan yang ada, melainkan sebagai penguat dalam kerangka autentikasi digital yang terstruktur dan berlapis. Dalam konteks *mobile banking*, penerapan *biometric authentication* sebagai bagian dari autentikasi berlapis dapat meningkatkan keamanan sistem secara keseluruhan. Biometrik berperan sebagai lapisan tambahan yang memperkuat proses verifikasi identitas, tanpa menghilangkan faktor autentikasi yang sudah ada. Selain aspek keamanan, NIST juga menekankan pentingnya keseimbangan antara tingkat perlindungan dan kemudahan penggunaan. Biometrik dipandang mampu meningkatkan keamanan sekaligus menjaga kenyamanan pengguna, karena proses autentikasi dapat dilakukan dengan cepat dan efisien tanpa ketergantungan penuh pada input manual seperti PIN atau *password*.

Maka implementasi sistem keamanan berbasis *biometric* pada aplikasi *mobile banking* merupakan upaya meningkatkan keamanan dan kenyamanan pengguna. Meskipun menghadapi berbagai tantangan, seperti masalah privasi dan kompatibilitas teknologi, potensi manfaat yang ditawarkan oleh *biometric* membuatnya menjadi pilihan yang menarik bagi penyedia layanan keuangan. Dengan perkembangan teknologi yang terus berlanjut dan peningkatan kesadaran akan pentingnya keamanan dalam dunia digital, teknologi biometric kemungkinan akan semakin banyak diadopsi dan dikembangkan di masa depan. Oleh karena itu, penting untuk terus melakukan penelitian dan pengembangan dalam bidang ini, guna mengoptimalkan penerapan teknologi biometric dan memastikan bahwa teknologi ini dapat memberikan manfaat yang maksimal bagi semua pihak yang terlibat.

2. Metode Penelitian

Dalam penelitian ini menggunakan metode penelitian deskriptif kualitatif. Peneliti hanya memaparkan situasi atau peristiwa. Tidak mencari hubungan, tidak menguji hipotesis atau membuat prediksi. Penelitian ini dilaksanakan di BSI KC Bukittinggi Sudirman, Kec. Aur Birugo Tigo Baleh, Kota Bukittinggi, Sumatera Barat. Informan yang berjumlah 5 orang yang terdiri dari 1 Manajer Operasional, 1 Customer Service, 3 Nasabah Pengguna *Mobile Banking*, yang dipilih menggunakan teknik purposive sampling, yaitu metode pemilihan informan secara sengaja berdasarkan kriteria tertentu yang relevan dengan tujuan penelitian. Pengumpulan data yang dilakukan melalui yaitu : 1) wawancara mendalam adalah suatu cara mengumpulkan data atau informasi dengan cara langsung bertatap muka dengan informan agar mendapatkan data lengkap dan mendalam; 2) Studi kepustakaan adalah proses pengumpulan data yang berasal dari berbagai sumber pustaka seperti buku, jurnal, dan sumber lain yang relevan dengan topik yang sedang dibahas oleh penulis; dan 3) dokumentasi yaitu peneliti mengambil data-data dari catatan, dokumentasi, dalam hal ini dokumentasi diperoleh melalui dokumen- dokumen atau arsip-arsip. Kemudian melakukan analisis data dengan menggunakan model Miles dan Huberman. Dalam model Miles dan Huberman, aktivitas yang dilakukan adalah klasifikasi data, reduksi data, deskripsi data dan menarik kesimpulan. Berdasarkan langkah-langkah yang dilaksanakan dalam pengolahan data, maka analisis data yang dilaksanakan dalam penelitian ini adalah pengolahan data melalui analisis deskriptif kualitatif, yaitu data yang dikumpulkan berupa kata kata, gambar dan bukan angka-angka serta di jelaskan dengan kalimat sehingga data yang diperoleh dapat dipahami maksud dan maknanya.

3. Hasil dan Pembahasan

Hasil dan pembahasan diperoleh berdasarkan seluruh data yang telah dikumpulkan oleh peneliti, yaitu melalui wawancara mendalam, studi kepustakaan dan dokumentasi. Data informan yang didapat melalui wawancara mendalam dapat dilihat pada tabel berikut:

Tabel 1.3
Gambaran Informan

NO	NAMA	JENIS KELAMIN	PEKERJAAN
1	Rasyudi	Laki-Laki	Manajer Operasional
2	Mega Purmita Sari	Perempuan	Customer Service

DOI: https://doi.org/10.31004/riggs.v5i1.8230
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

3	Nurul Azizah	Perempuan	Nasabah
4	Wena Amelia	Perempuan	Nasabah
5	Nadia Pasaribu	Perempuan	Nasabah

Dari tabel 4.1 di atas dapat diketahui bahwa informan berjumlah 5 orang, diantara 1 dari 5 informan berjenis kelamin laki-laki, dimana berarti 4 informan berjenis kelamin perempuan. Jadi dapat diketahui dengan jelas mayoritas informan adalah perempuan.

Implementasi Teknologi Biometric Authentication Terhadap Keamanan Pada Transaksi Nasabah Pengguna Mobile Banking

1. Implementasi Biometrik Pada Saat Pembukaan Rekening

Teknologi biometrik memainkan peran kunci dalam menjaga integritas data pengguna. Dengan melakukan identifikasi berbasis fitur fisik unik pengguna, seperti sidik jari, bank dapat memastikan bahwa setiap transaksi dilakukan oleh individu yang sah dan terverifikasi. Hal ini tidak hanya melindungi nasabah dari potensi pencurian identitas atau penipuan, tetapi juga memberikan kepastian bahwa data pribadi mereka aman dan terjaga dengan baik. Hal ini sesuai dengan hasil wawancara bahwa Teknologi Biometric yang digunakan pada *mobile banking* pada BSI yang disebut Byond sejauh ini efektif dan aman dalam meningkatkan keamanan. Dengan menghubungkan data biometrik nasabah dengan *database* Dukcapil, sistem dapat memastikan kesamaan postur wajah dan keaslian identitas nasabah. Selain itu, fitur seperti kedipkan mata dan gerakan kepala membuat sistem lebih sulit untuk ditipu dengan foto atau rekaman. Informan juga menyebutkan bahwa proses perekaman khususnya wajah, akan direkam ulang apabila aplikasi dihapus dan dipasang kembali. Informan juga menyampaikan bahwa ketika aplikasi diinstal ulang, sistem akan meminta pengguna untuk melakukan perekaman wajah kembali melalui proses *face registration*. Hal ini berarti bahwa setiap kali pengguna menghapus dan memasang ulang aplikasi, proses autentikasi biometrik harus dilakukan kembali sejak awal. Informan juga menegaskan bahwa yang dapat dilakukan penutupan hanyalah akses aplikasi atau layanan tertentu, sementara data rekening tetap ada selama rekening tersebut belum ditutup. Dengan demikian, meskipun aplikasi dapat dihapus atau ditutup sementara, pengguna tetap harus melalui tahapan perekaman biometrik ulang ketika ingin kembali menggunakan layanan mobile banking. Proses ini dipahami sebagai bagian dari mekanisme keamanan untuk memastikan bahwa pengguna yang mengakses aplikasi benar-benar merupakan pemilik sah rekening.

2. Implementasi Biometrik Pada Saat Membuka Aplikasi (Login)

Untuk masuk ke halaman utama aplikasi Byond, memerlukan *face id* ataupun *password* sebagai syarat keamanan login dan transaksi. Jika *face id* terdeteksi dan cocok dengan pemilik akun seperti tanda pada arah panah maka aplikasi akan otomatis masuk ke dalam menu utama.

Fasilitas login aplikasi Byond By BSI yang memanfaatkan fitur keamanan yang terdapat pada smartphone dimana aplikasi Byond By BSI tersebut terinstal. Fitur keamanan tersebut antara lain: konfirmasi wajah, sidik jari, kata sandi, *automatic closed*. Berikut Langkah-Langkah mengaktifkan biometrik Byond BSI:

a) Buka aplikasi Byond BSI
b) Login masukkan kata sandi
c) Klik profil pojok kanan
d) Login dan keamanan
e) Klik *Password* Biometrik

Mengaktifkan biometrik pada aplikasi Byond BSI melalui pengaturan aplikasi, sebaiknya tidak mengunduh aplikasi dari luar Play Store, App Store dan Store resmi lainnya, apalagi .APK dari pesan *Whatsapp/Telegram.*

3. Implementasi Biometrik Pada Saat Transaksi

Dalam *mobile banking* Byond terdapat penerapan sidik jari digunakan pada beberapa menu seperti Info Rekening, Transfer, Bayar, Beli, Berbagi-Ziswaf, Tarik Tunai, *Top-Up e-wallet* dan Qris.

Implementasi teknologi *biometric authentication* pada saat bertransaksi dalam layanan *mobile banking* diterapkan sebagai bagian dari mekanisme pengamanan berlapis. Pada sebagian perangkat, biometrik digunakan pada tahap awal untuk memastikan bahwa pengguna yang mengakses aplikasi merupakan pemilik sah rekening sebelum melakukan aktivitas transaksi. Proses ini dilakukan melalui verifikasi sidik jari atau pengenalan wajah, yang berfungsi sebagai bentuk konfirmasi identitas berbasis

DOI: https://doi.org/10.31004/riggs.v5i1.8230
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

karakteristik fisik pengguna. Dengan adanya tahapan ini, sistem dapat membatasi akses awal hanya kepada pengguna yang telah terdaftar dan tervalidasi secara biometrik.

Pada saat nasabah melakukan transaksi finansial, seperti transfer dana, sistem *mobile banking* tidak hanya mengandalkan biometrik, mekanisme ini dipahami sebagai bentuk pengamanan transaksi yang memiliki risiko finansial. Biometrik berperan untuk mengamankan akses ke aplikasi, sedangkan PIN digunakan sebagai konfirmasi akhir sebelum transaksi diproses. Implementasi ini menunjukkan bahwa biometrik difungsikan sebagai lapisan keamanan pendukung yang memperkuat proses autentikasi, tanpa menghilangkan peran faktor keamanan yang telah digunakan sebelumnya. Berarti implementasi biometrik tidak dimaknnai sebagai pengganti total metode keamanan, melainkan sebagai bagian dari sistem autentikasi berlapis dalam layanan. Peningkatan keamanan dalam penelitian ini tidak diartikan sebagai penghapusan seluruh resiko kejahatan digital, tetapi sebagai penambahan lapisan autentikasi, pengurangan peluang akses tidak sah, peningkatan proteksi akun nasabah. Biometrik meningkatkan keamanan ketika dikombinasikan dengan faktor lain, seperti PIN.

Meskipun biometrik tidak digunakan secara langsung untuk mengesahkan transaksi, keberadaannya tetap berkontribusi terhadap peningkatan keamanan karena menutup kemungkinan penyalahgunaan akun sejak tahap awal penggunaan aplikasi. Dengan demikian, implementasi biometrik pada transaksi mobile banking dapat dipahami sebagai upaya strategis untuk memperkuat sistem keamanan secara menyeluruh melalui pembatasan akses dan pengendalian otorisasi, bukan sekadar sebagai fitur tambahan yang berdiri sendiri.

Masalah Dan Tantangan Yang Dihadapi Dalam Implementasi Teknologi *Biometric* Pada Aplikasi *Mobile Banking*

1. Masalah Yang Dihadapi Dalam Implementasi Teknologi *Biometric* Pada Aplikasi *Mobile Banking*

a. Ketidakstabilan Verifikasi Biometrik

Berdasarkan wawancara yang dilakukan kepada informan bahwa terdapat kondisi di mana terkadang sistem gagal melakukan verifikasi meskipun telah dicoba berulang kali. Masalah ini menunjukkan bahwa keandalan teknologi biometrik masih bergantung pada kesiapan sistem aplikasi dan mekanisme autentikasi yang digunakan. Ketika kegagalan verifikasi terjadi, fungsi biometrik yang seharusnya meningkatkan efisiensi justru dapat menimbulkan ketidaknyamanan bagi pengguna. Fitur biometrik yang seharusnya dirancang untuk mempermudah nasabah dalam melakukan verifikasi justru terkadang menjadi sering kali gagal berfungsi. Menurut pernyataan nasabah sering mengalami situasi di mana proses verifikasi tidak berhasil meskipun sudah dicoba berkali-kali secara berulang. Masalah teknis ini muncul tanpa penyebab yang pasti, di mana nasabah merasa bingung apakah kendala tersebut berasal dari koneksi internet yang tidak stabil, adanya error pada sistem aplikasi, atau faktor teknis lainnya. Kondisi ini membuat fitur yang dimaksudkan untuk memberikan kepraktisan malah menjadi hambatan bagi nasabah dalam menggunakan layanan tersebut.

b. Ketergantungan Biometrik terhadap Kualitas Perangkat dan Jaringan

Keberhasilan autentikasi biometrik dalam *mobile banking* sangat dipengaruhi oleh kondisi teknis pendukung, seperti kualitas sensor sidik jari atau kamera pada perangkat, serta kestabilan koneksi internet. Berdasarkan wawancara, informan menduga bahwa kegagalan verifikasi biometrik dapat disebabkan oleh koneksi yang tidak stabil atau kualitas perangkat pengguna itu sendiri. Dari pernyataan nasabah ditemukan bahwa kendala dalam penggunaan biometrik tidak selalu bersumber dari sistem aplikasi perbankan, melainkan juga dipengaruhi oleh kondisi perangkat yang digunakan oleh nasabah.

Salah satu nasabah menyampaikan bahwa kondisi ponsel yang mengalami banyak goresan akibat pernah terjatuh menyebabkan proses verifikasi sidik jari tidak selalu berjalan dengan baik. Selain itu, nasabah juga menyebutkan adanya gangguan berupa kesalahan sistem saat memasukkan sidik jari, yang diperparah oleh kondisi memori perangkat yang penuh. Sehingga ini menunjukkan bahwa efektivitas implementasi biometrik juga sangat bergantung pada kualitas perangkat keras, seperti sensor sidik jari dan layar, serta kinerja perangkat secara keseluruhan. Ketika perangkat tidak berada dalam kondisi optimal, proses autentikasi biometrik berpotensi mengalami kegagalan meskipun sistem keamanan aplikasi telah dirancang dengan baik.

DOI: https://doi.org/10.31004/riggs.v5i1.8230
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Dengan demikian, dari hasil wawancara mengindikasikan bahwa ketergantungan biometrik terhadap kualitas perangkat dan jaringan nasabah menjadi salah satu permasalahan internal dalam implementasi teknologi ini, karena keberhasilan autentikasi tidak hanya ditentukan oleh sistem perbankan, tetapi juga oleh kesiapan dan kondisi perangkat yang digunakan oleh pengguna.bekerja secara optimal tanpa dukungan infrastruktur atau perangkat sistem yang memadai. Dengan demikian, efektivitas biometrik tidak hanya ditentukan oleh aplikasi itu sendiri, tetapi juga oleh kondisi teknis yang berada dalam sistem internal perangkat pengguna.

c. Biometrik Belum Digunakan Sebagai Pengaman Penuh pada Seluruh Tahapan Transaksi

Meskipun biometrik telah diterapkan, sistem transaksi tetap mengandalkan PIN dan *password* sebagai bentuk pengamanan lanjutan. Ketika nasabah tidak menjaga kerahasiaan dan membagikannya kepada pihak lain, sistem tetap akan memproses transaksi sebagai sah.

Berdasarkan pernyataan informan bahwa proses transaksi dalam *mobile banking* tetap menggunakan PIN dan *password*, sementara biometrik hanya diterapkan pada tahap registrasi atau akses awal, dapat diidentifikasi adanya keterbatasan dalam pemanfaatan biometrik sebagai mekanisme pengamanan penuh. Kondisi ini menunjukkan bahwa peran biometrik masih bersifat pendukung dan belum diintegrasikan secara langsung dalam proses otorisasi transaksi. Akibatnya, keamanan transaksi masih sangat bergantung pada kerahasiaan PIN dan *password* yang bersifat *knowledge-based*, yang berpotensi diketahui atau dibagikan kepada pihak lain. Pendapat ini dapat dipandang sebagai salah satu masalah dalam implementasi biometrik, karena meskipun teknologi biometrik telah diterapkan, perlindungan pada tahap transaksi belum sepenuhnya memanfaatkan keunggulan biometrik sebagai identitas unik pengguna.

Dengan demikian, penggunaan biometrik yang terbatas pada tahap registrasi atau login saja menunjukkan bahwa sistem keamanan *mobile banking* masih menyisakan celah pada fase transaksi, sehingga tujuan peningkatan keamanan melalui biometrik belum optimal sepenuhnya.

2. Tantangan Yang Dihadapi Dalam Implementasi Teknologi *Biometric* Pada Aplikasi *Mobile Banking*

a. Rendahnya Literasi Digital Pada Sebagian Nasabah, Khususnya Usia Lanjut dan Tingkat Pendidikan Terbatas

Berdasarkan hasil wawancara tersebut, rendahnya literasi digital merupakan tantangan besar yang mencakup seluruh lapisan nasabah dalam berinteraksi dengan layanan perbankan. Masalah utama terletak pada perilaku nasabah yang sering kali kurang waspada dalam memproses informasi, seperti secara sembarangan mengeklik tautan atau mengisi data pribadi tanpa memahami konsekuensinya, terutama saat berhadapan dengan nasabah dari generasi *baby boomers* atau lansia. Pihak bank mengakui bahwa mengedukasi kelompok usia lanjut ini memang terasa agak susah dan memberikan tantangan tersendiri pada tahap awal karena mereka memerlukan waktu lebih untuk memahami sistem yang ada. Meskipun tantangan ini terasa berat di awal, tingkat kesulitan tersebut biasanya akan berkurang setelah nasabah mulai paham dan terbiasa dengan teknologi yang digunakan. Selain itu juga nasabah dengan tingkat pendidikan relatif rendah dengan keterbatasan pemahaman terhadap istilah teknis, risiko keamanan digital, serta konsekuensi dari kebocoran data menyebabkan sebagian nasabah kurang menyadari pentingnya menjaga keamanan data. Ini menunjukkan bahwa tantangan implementasi *biometric authentication* tidak hanya bersumber dari aspek teknologi, tetapi juga dari faktor manusia dan kondisi teknis.

b. Perilaku Nasabah dalam Menjaga Keamanan Data Autentikasi

Tantangan eksternal lain yang diungkapkan dalam wawancara berkaitan juga dengan perilaku nasabah yang kurang menjaga kerahasiaan PIN. Informan menjelaskan bahwa sebagian besar kasus transaksi bermasalah bukan hanya disebabkan oleh kegagalan sistem atau biometrik, melainkan karena PIN diketahui oleh orang lain, seperti anggota keluarga. Kondisi ini menunjukkan bahwa tingkat keamanan *mobile banking* tidak hanya ditentukan oleh teknologi, tetapi juga oleh kesadaran dan tanggung jawab pengguna dalam melindungi data autentikasinya.

Pihak bank secara rutin melakukan edukasi kepada masyarakat melalui layanan *Customer*

DOI: https://doi.org/10.31004/riggs.v5i1.8230
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Service (CS) dan media sosial untuk menekankan pentingnya menjaga kerahasiaan PIN sebagai lapisan keamanan utama. Tantangan yang dihadapi dalam perilaku nasabah adalah kesadaran untuk tidak memberikan data autentikasi, seperti PIN dan kata sandi, kepada siapapun, termasuk kepada petugas bank sekalipun. Risiko keamanan muncul bukan hanya saat perangkat fisik seperti ponsel hilang, namun justru ketika nasabah secara tidak sadar membagikan PIN mereka, yang memungkinkan pihak lain untuk melakukan transaksi tanpa izin. Oleh karena itu, tantangan bank adalah memastikan nasabah tetap disiplin menjaga kerahasiaan data tersebut, karena sistem keamanan hanya akan efektif selama PIN tetap menjadi informasi yang eksklusif diketahui oleh nasabah itu sendiri.

c. Ancaman Fishing di Luar Sistem Bank

Dari hasil wawancara juga mengungkapkan bahwa biometrik tidak mampu sepenuhnya melindungi nasabah dari ancaman Fishing dan manipulasi sosial. Ketika nasabah mengklik tautan mencurigakan atau memberikan data pribadi kepada pihak yang tidak berwenang, risiko penyalahgunaan akun tetap dapat terjadi. Tantangan ini berada di luar kendali langsung sistem biometrik dan menunjukkan bahwa implementasi teknologi keamanan perlu disertai dengan edukasi berkelanjutan kepada nasabah terkait ancaman kejahatan digital. Dalam penjelasannya, informan menekankan bahwa keamanan dana nasabah sangat bergantung pada kewaspadaan pribadi dalam menghadapi "umpan" yang diberikan oleh penipu. Selama nasabah tidak mengeklik tautan mencurigakan atau memberikan data sensitif (seperti PIN dan kata sandi) kepada pihak mana pun termasuk petugas bank maka akun mereka akan tetap aman. Namun, jika nasabah terlanjur berinteraksi dengan tautan tersebut dan mengisi data pribadi, hal itu berada di luar kewenangan dan tanggung jawab bank. Oleh karena itu, nasabah dihimbau untuk selalu memverifikasi informasi yang meragukan melalui tautan resmi, seperti *call center* di 14040, media sosial resmi, atau situs web resmi bank.

Maka salah satu risiko utama terjadinya pencurian data pribadi yang berujung pada *fishing* adalah perbedaan tingkat kesadaran dan pemahaman nasabah mengenai praktik keamanan yang baik, seperti penggunaan kata sandi yang kuat dan berhati-hati dalam mengklik tautan mencurigakan, serta menggarisbawahi pentingnya edukasi yang efektif.

Dampak Implementasi Teknologi Biometric Terhadap Keamanan Nasabah Pengguna Mobile Banking Dalam Melakukan Transaksi

1. Meningkatkan Persepsi Keamanan dan Kenyamanan

Penggunaan fitur biometrik dalam layanan *mobile banking* menurut nasabah merupakan mekanisme keamanan yang mampu memberikan rasa aman yang cukup tinggi. Salah satu informan menyampaikan bahwa perbedaan karakteristik biometrik setiap individu, seperti sidik jari dan wajah, menjadi alasan utama munculnya keyakinan bahwa akun sulit diakses oleh pihak lain. Pernyataan ini menunjukkan bahwa nasabah memahami biometrik sebagai identitas personal yang tidak mudah ditiru, sehingga memberikan perlindungan tambahan terhadap akses tidak sah. Meskipun informan menyadari masih terdapat sedikit kekhawatiran, keyakinan tersebut tetap dominan dan membentuk persepsi bahwa sistem keamanan yang diterapkan sudah cukup memadai.

Pandangan tersebut diperkuat oleh pernyataan informan lain yang menegaskan bahwa kombinasi antara sidik jari dan PIN semakin membatasi kemungkinan orang lain untuk membuka akun. Informan menyebutkan bahwa keberadaan dua lapisan keamanan tersebut membuat akses terhadap aplikasi menjadi lebih aman. Hal ini menunjukkan bahwa nasabah tidak memandang biometrik sebagai pengganti PIN, melainkan sebagai pelengkap yang memperkuat sistem keamanan. Persepsi ini sejalan dengan pemahaman bahwa keamanan digital tidak hanya bergantung pada satu mekanisme, tetapi pada kombinasi beberapa metode autentikasi.

Selain aspek keamanan, hasil wawancara juga menunjukkan bahwa penerapan biometrik memberikan dampak langsung terhadap kenyamanan dan kemudahan nasabah dalam melakukan transaksi digital. Informan menyampaikan bahwa penggunaan biometrik dirasakan lebih praktis dibandingkan penggunaan password yang panjang dan kompleks. Rasa aman dan nyaman yang dirasakan nasabah saling berkaitan dan saling memperkuat. Ketika nasabah merasa aman, mereka

DOI: https://doi.org/10.31004/riggs.v5i1.8230
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

cenderung merasa nyaman dalam menggunakan layanan. Sebaliknya, kemudahan dan kenyamanan penggunaan biometrik memperkuat persepsi bahwa sistem aman dan dapat diandalkan.

2. Mengurangi Kekhawatiran Nasabah Terhadap Penyalahgunaan Akun

Informan pertama menyatakan bahwa keberadaan biometrik membuat akun menjadi lebih sulit dibajak. Pernyataan ini mencerminkan pemahaman nasabah bahwa biometrik menghadirkan mekanisme keamanan yang tidak hanya bergantung pada informasi yang dapat diingat atau diketahui oleh orang lain, seperti PIN, tetapi juga pada karakteristik fisik unik yang melekat pada pemilik akun. Persepsi ini penting karena menunjukkan bahwa biometrik dipandang sebagai bentuk perlindungan yang bersifat personal dan sulit ditiru.

Pendapat tersebut diperkuat oleh pernyataan informan lain yang menegaskan bahwa kombinasi antara sidik jari dan PIN membuat akses terhadap akun *mobile banking* menjadi semakin terbatas. Informan tidak hanya menyoroti keberadaan biometrik semata, tetapi juga menekankan bahwa keamanan yang lebih tinggi tercipta dari penggunaan biometrik yang dibarengi dengan PIN. Hal ini menunjukkan bahwa nasabah memahami konsep keamanan berlapis, meskipun dalam bahasa yang sederhana. Menurut mereka, akses terhadap akun tidak dapat dilakukan dengan mudah karena memerlukan dua bentuk verifikasi yang berbeda, sehingga peluang orang lain untuk masuk ke akun menjadi semakin kecil.

Selanjutnya, pernyataan dari informan lain kembali menegaskan bahwa meskipun perangkat seperti handphone berada di tangan orang lain atau bahkan hilang, risiko penyalahgunaan akun tetap dianggap kecil. Informan mengaitkan hal ini dengan adanya sidik jari dan pengenalan wajah yang hanya dimiliki oleh pemilik akun. Selain itu, informan juga menyebutkan bahwa PIN tetap menjadi faktor penting karena hanya diketahui oleh pemilik akun. Pernyataan ini menunjukkan bahwa nasabah melihat biometrik bukan sebagai satu-satunya pengaman, melainkan sebagai penguat sistem keamanan yang sudah ada. Dengan kata lain, biometrik dipersepsikan sebagai mekanisme yang melengkapi dan memperkuat perlindungan akun, bukan menggantikannya.

Secara keseluruhan menggambarkan bahwa implementasi biometrik dalam *mobile banking* memberikan merasa bahwa risiko pembajakan akun menjadi lebih kecil karena akses tidak hanya bergantung pada satu faktor keamanan. Pendapat ini berkontribusi pada meningkatnya kepercayaan nasabah terhadap sistem keamanan yang diterapkan oleh bank. Dengan demikian, meskipun transaksi tetap memerlukan PIN, keberadaan biometrik dinilai mampu meningkatkan keamanan secara keseluruhan dengan membatasi akses awal dan mempersulit pihak yang tidak berwenang untuk menggunakan akun *mobile banking*.

3. Meningkatkan Kepercayaan Nasabah terhadap Bank

Penerapan fitur biometrik dalam layanan *mobile banking* tidak hanya dipersepsikan sebagai bentuk peningkatan keamanan teknis, tetapi juga sebagai wujud komitmen bank dalam menjaga privasi dan data pribadi nasabah. Salah satu informan menyampaikan bahwa dengan adanya fitur biometrik, ia merasa pihak bank telah berupaya secara serius untuk memberikan perlindungan terhadap data pribadinya. Pendapat tersebut kemudian berdampak langsung pada meningkatnya tingkat kepercayaan nasabah terhadap bank. Informan menyatakan bahwa kehadiran fitur ini membuatnya yakin bahwa bank tidak mengabaikan aspek keamanan, sehingga rasa percaya terhadap pengelolaan data pribadi pun semakin kuat. Pandangan tersebut diperkuat oleh pernyataan informan lain yang menekankan bahwa kepercayaan muncul karena data pribadi dianggap hanya diakses oleh pihak yang berkepentingan, yakni antara nasabah dan bank. Hal ini menunjukkan bahwa nasabah memandang biometrik sebagai mekanisme yang membatasi akses data secara lebih ketat dibandingkan metode konvensional. Pendapat ini memperlihatkan bahwa keamanan tidak hanya diartikan sebagai perlindungan dari pembajakan akun, tetapi juga sebagai jaminan bahwa data pribadi tidak disalahgunakan atau diakses oleh pihak lain tanpa izin. Dengan demikian, hasil wawancara ini menggambarkan bahwa biometrik berperan dalam membangun hubungan kepercayaan antara nasabah dan bank, di mana rasa aman terhadap data pribadi dan sistem aplikasi menjadi faktor penting dalam meningkatkan kepercayaan nasabah terhadap layanan *mobile banking*.

DOI: https://doi.org/10.31004/riggs.v5i1.8230
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

4. Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan bahwa implementasi teknologi biometric authentication pada layanan *mobile banking* telah berkontribusi dalam memperkuat keamanan akses nasabah, khususnya pada tahap pembukaan rekening digital dan login aplikasi. Biometrik diyakini mampu memberikan rasa aman dan kenyamanan karena berbasis pada identitas personal yang sulit ditiru. Namun demikian, pada tahap transaksi keuangan, biometrik belum diterapkan sebagai mekanisme pengamanan utama dan masih dikombinasikan dengan PIN atau *password*. Kondisi ini menunjukkan bahwa biometrik berfungsi sebagai lapisan pengamanan tambahan, bukan sebagai sistem yang berdiri sendiri. Selain itu, efektivitas implementasi biometrik juga dipengaruhi oleh berbagai faktor, baik dari dalam sistem maupun dari luar, seperti keterbatasan teknis aplikasi, kondisi perangkat dan jaringan nasabah, serta tingkat literasi digital. Meskipun masih terdapat keterbatasan tersebut, secara umum teknologi biometrik memberikan dampak positif terhadap persepsi keamanan dan kepercayaan nasabah dalam menggunakan layanan *mobile banking*.

Referensi

1. Arifianto, Teguh, 'Penerapan Fingerprint Recognition Dengan Metode Learning Vector Quantization (LVQ) Dalam Automatic Teller Machine (ATM)', Spirit : STMIK Yadika Journal of Computing and Cybernetic System, 9.2 (2017), pp. 8–13
2. Basuki, Ferry Hendro, 'Analisis Swot Financial Technology Pada Dunia Perbankan Di Kota Ambon', Jurnal Manis, Vol 2.No 1 (2018), p. 65
3. Burhanuddin, Agussalim, Studi Keamanan (UNHAS, 2017)
4. Dermawan, Irwan, and others, 'Serangan Cyber Dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia', *Jurnal Informasi Dan Teknologi*, 5.3 (2023), pp. 20–25, doi:10.60083/jidt.v5i3.364
5. Khan, M A, *Theory and Practice of Insurance* (Educational Book House, 1983) <https://books.google.co.id/books?id=V7qeAQAACAAJ>
6. Kriyantono, Rachmat, *Teknik Praktis Riset Komunikasi* (Kencana Prenadamedia Group, 2016)
7. Nugratama, Aufar, and others, Financial Technology (Lauk Puyu Press, 2025) <https://www.researchgate.net/publication/395731161_Financial_Financial_Technology_Technology
8. Otoritas Jasa Keuangan (OJK), 'Penguatan Sektor Jasa Keuangan Dalam Menjaga Pertumbuhan Ekonomi: Laporan Kinerja OJK Tahun 2023', 2024, pp. 1–292 <https://www.ojk.go.id/id/data-dan-statistik/laporan-tahunan/Documents/Laporan Tahunan OJK 2023_.pdf>
9. Rachmat, Jalaludin, *Metode Penelitian Komunikasi* (PT. Remaja Rosda Karya, 2005)
10. Saputri, Vettyca Diana, 'Implementation Of Biometric-Based Security System On Mobile Banking Application', Jurnal Komputer Indonesia, 2.1 (2023), pp. 25– 32, doi:10.37676/jki.v2i1.565
11. Sari, Dwi Mutiara, Muhammad Iqbal Fasa, and Suharto Suharto, 'Fitur-Fitur Aplikasi Mobile Banking Bank Syaraih', Al-Infaq: Jurnal Ekonomi Islam, 12.2 (2021), p. 170 <https://jurnalfai- uikabogor.org/index.php/alinfaq/article/view/892/603>
12. Sarwoko, Eko Adi, 'Mekanisme Sistem Identifikasi Biometrik', Prosiding Seminar Nasional SPMIPA 2006, 2006, pp. 3–6
13. Studi, Program, Teknik Informatika, and Fakultas Teknologi Informasi, 'Penerapan Sistem Biometrik Pada Nasabah Pengguna ATM (Studi Kasus IKPIA Perbanas Jakarta)', pp. 1042–47
14. Sulistyorini, Siska, 'Teori-Teori Implementasi Dan Adopsinya Dalam Pendidikan', no. November (2022)
15. Sumijan, Pradani Ayu, and Arlis Syafri, Teknologi Biometrik Impementasi Pada Bidang Medis Menggunakan Matlabs, Teknologi Biometrik, 2021
16. Syariah, Fakultas, and others, 'Pengawasan Bank Indonesia Atas Kerahasiaan Dan Keamanan Data / Informasi Konsumen Financial Technology Pada Sektor Mobile', 11.1, pp. 16–47, doi:10.18860/j.v11i1.5829
17. Tarigan, Joshua, 'Biometric Security : Alternatif Pengendalian Dalam Sistem', *Jurnal Akuntansi & Keuangan*, 6.2 (2004), pp. 90–105 <http://jurnalakuntansi.petra.ac.id/index.php/aku/article/view/16156>
18. Temoshok, David, and others, *NIST Special Publication Authentication and Authenticator Management NIST SP 800-63B-4 Authentication and Authenticator Management*
19. Utami, Zulfa, 'Analisis Penggunaan Teknologi Biometrik Dalam Sistem Keamanan Dan Identifikasi Pengguna', Cyberarea.Id, 3.5 (2023), pp. 1–17 <http://cyberarea.id/index.php/cyberarea/issue/view/20>
20. Yeovandi, Felix, Sabariman Sabariman, and Stefanus Eko Prasetyo, 'Evaluasi Keamanan Sistem Autentikasi Biometrik Pada Smartphone Dan Rekomendasi Implementasi Optimal', JTIM : Jurnal Teknologi Informasi Dan Multimedia, 7.1 (2025), pp. 133–48, doi:10.35746/jtim.v7i1.653
21. Yogyakarta, P3EI UII, Ekonomi Islam (Rajawali Press, 2012)
22. Yudhira, Ahmad, 'Value Jurnal Ilmiah Akuntansi Keuangan Dan Bisnis Analisis Perkembangan Financial Technology (Fintech) Syariah Pada Masa Pandemi Covid-19 Di Indonesia', Value Jurnal Ilmiah Akuntansi Keuangan Dan Bisnis, 1.2 (2021), pp. 13–28
23. Zulaikah, Salma Mufatikhaturrohmah dan, 'Pengaruh Teknologi Biometrik Dan Jaminan Keamanan Cyber Terhadap Minat Transaksi Perbankan Online Di Provinsi Lampung Dalam Perspektif Islam', Jurnal Informatika Ekonomi Bisnis, 7 (2025), doi:10.37034/infeb.v7i2.1136
24. Yang, Wencheng, and others, *Biometrics for Internet-of-things Security: A Review*, *Sensors*, 2021, XXI, doi:10.3390/s21186163

DOI: https://doi.org/10.31004/riggs.v5i1.8230
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)