

## STUDI LITERATUR SISTEM KEAMANAN BIOMETRIK UNTUK VERIFIKASI MOBILE BANKING BANK SYARIAH

Adilla Nadzifatuz Zahra<sup>1</sup>, Khairul Umam Khudhori<sup>2</sup>, Ranaswijaya<sup>3</sup>, Apriyani Lestari<sup>4</sup>

<sup>1,2,3,4</sup>Institut Agama Islam Negeri Curup

<sup>1</sup>[adillanadzifatuz12@gmail.com](mailto:adillanadzifatuz12@gmail.com), <sup>2</sup>[khairulumamkhudhori@gmail.com](mailto:khairulumamkhudhori@gmail.com),

<sup>3</sup>[ranaswijaya@iaincurup.ac.id](mailto:ranaswijaya@iaincurup.ac.id), <sup>4</sup>[Apriyani8423@gmail.com](mailto:Apriyani8423@gmail.com)

Received: 08-10- 2025

Revised: 18-10-2025

Approved: 15-11-2025

### ABSTRAK

*Penelitian ini bertujuan untuk menganalisis penerapan sistem keamanan biometrik dalam verifikasi mobile banking pada bank syariah serta mengevaluasi efektivitas, tantangan, dan relevansinya berdasarkan perspektif keamanan, prinsip syariah, dan regulasi hukum positif. Metode penelitian yang digunakan adalah studi literatur dengan pendekatan deskriptif kualitatif, yang menelaah berbagai referensi ilmiah, dokumen hukum, hasil penelitian terdahulu, serta data implementasi biometrik pada bank syariah di Indonesia seperti BSI, BCA Syariah, dan Bank Mega Syariah. Hasil penelitian menunjukkan bahwa teknologi biometrik memberikan tingkat keamanan yang lebih tinggi dibandingkan metode tradisional seperti PIN dan OTP karena berbasis ciri biologis yang unik, sulit dipalsukan, dan praktis digunakan. Penerapan biometrik juga dinilai sesuai dengan prinsip *hifz al-mal* dalam *maqashid syariah* dan didukung oleh regulasi hukum seperti Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022). Namun, implementasi biometrik menghadapi tantangan berupa risiko kebocoran data, ketergantungan teknologi perangkat, dan isu etika privasi. Simpulan penelitian ini menunjukkan bahwa biometrik efektif meningkatkan keamanan verifikasi mobile banking bank syariah, namun perlu diimbangi dengan perlindungan hukum, edukasi nasabah, dan dukungan infrastruktur teknologi agar implementasinya optimal, aman, dan sesuai prinsip syariah.*

**Kata Kunci:** Biometrik, Mobile Banking, Keamanan Data, Bank Syariah, Verifikasi

### PENDAHULUAN

Menurut Bank Indonesia, teknologi finansial adalah pemanfaatan teknologi dalam sistem keuangan untuk menciptakan produk, layanan, teknologi, dan model bisnis baru, serta meningkatkan stabilitas mata uang, stabilitas sistem keuangan, efisiensi, kelancaran, keamanan, dan kepercayaan terhadap sistem pembayaran (Hendra Kusuma & Wiwiek Kusumaning Asmoro, 2020). Dengan kata lain, teknologi finansial adalah pemanfaatan teknologi di bidang keuangan untuk menyediakan layanan pembayaran. Keberadaan dompet elektronik (e-wallet), yang merupakan bagian dari sistem pembayaran elektronik, kini memungkinkan pengguna dengan mudah melakukan pembayaran, membeli pulsa, dan melakukan transaksi lainnya (Hendra Kusuma & Wiwiek Kusumaning Asmoro, 2020). Istilah dompet elektronik mengacu pada bentuk dompet digital yang memungkinkan pengguna menghubungkan kartu debit atau kredit mereka ke dompet digital untuk melakukan transaksi. Selain kartu debit dan kredit, dompet elektronik memungkinkan konsumen menyimpan informasi kartu fisik dan nomor rekening bank untuk menyelesaikan transaksi tertentu. Namun, muncul pertanyaan tentang bagaimana menyediakan otentikasi pengguna. Otentikasi adalah proses mengidentifikasi pengguna terdaftar atau dikenal untuk diberikan layanan tertentu dan melindungi informasi pengguna dari penyusup (Hartono, Rizaldy & Lestari, 2022).

Ada dua alasan utama mengapa keamanan dibutuhkan: pertama, untuk mengidentifikasi pengguna yang berwenang, dan kedua, untuk melindungi privasi. Keamanan tradisional pada dompet digital menggunakan PIN dan OTP (One Time Password) untuk otentikasi setiap transaksi (Putri & Fahrozi, 2021). Saat ini teknologi

biometrik telah digunakan dalam proses otentikasi, yaitu teknologi yang memanfaatkan ciri biologis seseorang seperti sidik jari, telapak tangan, wajah, atau iris mata. Setiap individu memiliki karakteristik biologis yang unik, bahkan kembar identik pun memiliki perbedaan. Oleh karena itu, teknologi ini dipercaya memberikan keamanan yang lebih tinggi karena sulit untuk dipalsukan (Kusuma, 2023). Namun, kelemahan dari teknologi biometrik adalah biaya implementasinya yang tinggi, proses identifikasinya yang lambat, serta terkadang kurang dapat diandalkan. Meskipun demikian, teknologi ini tetap memberikan tingkat perlindungan tertinggi dibandingkan metode lainnya (Kusuma, 2023). Perbankan sebagai industri yang mengutamakan kepuasan nasabah dalam seluruh layanan terus mengembangkan teknologi untuk memastikan layanan yang diberikan tetap aman dan mudah diakses oleh nasabah (Adinugraha & Sartika, 2020). Bentuk layanan perbankan berbasis teknologi di antaranya adalah electronic banking (e-banking), yang mencakup mobile banking, internet banking, dan SMS banking (Firjatullah et al., 2021).

Menurut Otoritas Jasa Keuangan (POJK No. 12/POJK.03/2018), layanan perbankan digital adalah layanan yang disediakan melalui media elektronik dengan mengoptimalkan penggunaan data nasabah. Meskipun jumlah transaksi digital di Indonesia mengalami fluktuasi, tren jangka panjang menunjukkan peningkatan penggunaan layanan digital banking dalam lima tahun terakhir (Putra et al., 2023). Selain memberikan kemudahan, bank juga memiliki tanggung jawab untuk menjamin keamanan data nasabah dari berbagai aktivitas kriminal digital, seperti pencurian data atau peretasan sistem. Menurut Budhi Hardjo, keamanan informasi adalah upaya untuk mendeteksi dan mencegah aktivitas penipuan pada sistem informasi, terutama karena informasi digital tidak berbentuk fisik sehingga rawan disalahgunakan (Putri & Fahrozi, 2021). Bank pada umumnya menggunakan sistem keamanan berupa *password* dan PIN yang dibuat oleh nasabah. Namun, metode ini masih memiliki kelemahan dan risiko terhadap kejahatan siber seperti pencurian data melalui internet. Hal ini menunjukkan perlunya sistem keamanan baru yang lebih kuat, seperti biometrik.

Seiring meningkatnya mobilitas masyarakat dan aktivitas transaksi digital, bank syariah dituntut tidak hanya memberikan kemudahan akses finansial, tetapi juga memastikan keamanan dan kepercayaan nasabah. Kejahatan siber seperti *phishing*, *skimming*, hingga *data breach* semakin berkembang dan menargetkan nasabah mobile banking, termasuk pada perbankan syariah. Berdasarkan laporan Otoritas Jasa Keuangan (OJK) tahun 2023, terdapat kenaikan kasus kejahatan siber di sektor jasa keuangan sebesar 27%, terutama pada layanan digital banking dan e-wallet (OJK, 2023). Kondisi ini membuktikan bahwa sistem keamanan tradisional seperti PIN dan OTP tidak lagi cukup, sehingga inovasi seperti biometrik menjadi kebutuhan yang semakin mendesak (Rahman & Purwanto, 2022). Penerapan teknologi biometrik dalam mobile banking bank syariah dinilai relevan untuk memperkuat sistem *authentication* dan *authorization*. Teknologi ini menggunakan ciri biologis yang unik seperti sidik jari, pengenalan wajah, atau iris mata yang sulit dipalsukan. Bank Syariah Indonesia (BSI), Bank Mega Syariah, dan BCA Syariah telah menerapkan fitur biometrik pada proses log in dan verifikasi transaksi untuk meningkatkan keamanan dan kenyamanan pengguna (Wulandari & Hidayat, 2023). Pengguna kini tidak hanya memasukkan PIN, tetapi cukup menggunakan sidik jari atau face recognition untuk mengakses akun mereka. Hal ini juga sejalan dengan kebutuhan generasi milenial dan Gen Z yang lebih menyukai layanan cepat, bebas ribet, dan tetap aman (Saputri et al., 2023).

Dari perspektif syariah, penerapan biometrik tidak bertentangan dengan prinsip

Islam. Justru, hal ini termasuk bagian dari penjagaan terhadap harta (hifz al-mal) dalam maqashid syariah. Sepanjang data biometrik disimpan dengan aman, tidak disalahgunakan, dan tidak mengandung unsur eksploitasi, maka hukumnya diperbolehkan (*mubah*), bahkan dianjurkan untuk mencegah kerugian dan tindakan kriminal (Hidayatullah, 2021). Oleh karena itu, integrasi biometrik dalam mobile banking syariah menjadi bagian penting dari inovasi modern yang tetap menjaga nilai-nilai syariah. Namun, sistem ini juga menghadapi tantangan besar dalam hal perlindungan data pribadi. Data biometrik termasuk kategori data spesifik dan sensitif menurut Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022). Artinya, bank wajib mendapatkan persetujuan nasabah, menjamin kerahasiaan data, serta mencegah penyalahgunaan atau akses ilegal terhadap data biometrik tersebut (Kominfo, 2023). Tanpa adanya regulasi dan pengawasan yang kuat, teknologi biometrik justru dapat menjadi ancaman baru apabila data nasabah bocor ke pihak yang tidak bertanggung jawab.

## **METODE PENELITIAN**

Penelitian ini menggunakan metode studi literatur dengan pendekatan deskriptif kualitatif, yang bertujuan untuk menganalisis, membandingkan, dan menginterpretasikan konsep serta temuan penelitian terdahulu terkait penerapan sistem keamanan biometrik dalam verifikasi mobile banking bank syariah. Pendekatan ini dipilih karena mampu memberikan pemahaman mendalam mengenai fenomena keamanan biometrik dalam perbankan digital syariah tanpa melakukan penelitian lapangan (Sugiyono, 2019; Zed, 2014). Jenis penelitian ini adalah deskriptif kualitatif, dengan fokus mengeksplorasi bagaimana teknologi biometrik diterapkan dalam mobile banking bank syariah serta menganalisis kelebihan, kelemahan, tantangan, dan relevansinya dengan prinsip syariah dan hukum positif. Sumber data yang digunakan bersifat sekunder, diperoleh dari:

- Jurnal ilmiah nasional dan internasional,
- Buku, prosiding, artikel ilmiah,
- Laporan resmi dari OJK, Bank Indonesia, dan Kementerian Kominfo,
- Dokumen hukum seperti Undang-Undang Perlindungan Data Pribadi dan Fatwa DSN-MUI.

Teknik pengumpulan data menggunakan metode dokumentasi, yaitu mengumpulkan, mengkaji, dan menyeleksi data tertulis yang relevan dengan topik sistem keamanan biometrik, mobile banking, dan perbankan syariah (Arikunto, 2013). Analisis data dilakukan melalui model analisis Miles dan Huberman, yang meliputi:

- 1) Reduksi Data  
Melakukan seleksi dan penyederhanaan data dari berbagai literatur dengan menyoroti aspek-aspek penting seperti:
  - a. Konsep biometrik dan penerapan pada mobile banking,
  - b. Keamanan, risiko, serta tantangan implementasi biometrik,
  - c. Perspektif syariah dan hukum terkait data biometrik,
  - d. Dampak biometrik terhadap keamanan dan kenyamanan nasabah.
- 2) Penyajian Data (Data Display)  
Data disajikan dalam bentuk deskriptif naratif dan tabel temuan untuk mengklasifikasikan fungsi biometrik, kelebihan, kekurangan, dan penerapannya pada bank syariah seperti BSI, BCA Syariah, dan Bank Mega Syariah.

3) Penarikan Kesimpulan

Menyimpulkan efektivitas penggunaan biometrik dalam mobile banking bank syariah, relevansi dengan maqashid syariah, serta implikasi terhadap keamanan data dan perlindungan nasabah.

Validitas data diperoleh melalui triangulasi sumber, yaitu melakukan perbandingan antara berbagai sumber ilmiah, dokumen hukum, dan praktik implementasi biometrik di bank syariah. Tujuan triangulasi adalah memastikan akurasi, konsistensi, serta kredibilitas informasi yang digunakan. Tahapan penelitian meliputi:

- Identifikasi dan penetapan fokus kajian.
- Pengumpulan referensi ilmiah dan dokumen terkait biometrik dan mobile banking syariah.
- Analisis dan sintesis isi literatur secara tematik.
- Penyusunan pembahasan dan kesimpulan berdasarkan data yang dianalisis.

Dengan metode ini, penelitian diharapkan mampu memberikan gambaran komprehensif dan mendalam mengenai penerapan sistem keamanan biometrik dalam verifikasi mobile banking bank syariah, sekaligus menilai efektivitas, tantangan, dan kesesuaiannya dengan prinsip syariah dan regulasi hukum positif di Indonesia.

#### HASIL PENELITIAN DAN PEMBAHASAN

Perkembangan teknologi berbanding lurus dengan perkembangan gaya hidup masyarakat saat ini. Semakin banyak informasi yang tersedia melalui berbagai media, baik cetak maupun elektronik, membuat masyarakat membutuhkan akses informasi yang cepat dan akurat untuk memenuhi kebutuhan sehari-hari. Kebutuhan akan mobilitas serta akses informasi yang praktis membuat gaya hidup masyarakat modern sangat erat kaitannya dengan penggunaan perangkat teknologi seperti smartphone dan internet (Fachmi & Setiawan, 2020). Pemanfaatan teknologi informasi juga sangat terasa dalam industri perbankan, baik bank konvensional maupun bank syariah. Salah satu bentuk pemanfaatan teknologi ini adalah layanan *mobile banking (m-banking)*, yang memungkinkan nasabah melakukan berbagai transaksi seperti transfer, pembayaran tagihan, pembelian pulsa, hingga pengecekan saldo tanpa harus datang ke kantor cabang atau ATM (Nurdin et al., 2021). Mobile banking bertujuan untuk meningkatkan efisiensi, kenyamanan, keamanan, dan kepuasan nasabah dalam bertransaksi. Perbankan syariah juga turut mengadopsi teknologi mobile banking dengan tetap memperhatikan prinsip-prinsip syariah dalam seluruh transaksinya, seperti penggunaan akad yang sesuai dengan hukum Islam dalam transfer, pembayaran, atau transaksi lainnya agar tidak bertentangan dengan prinsip syariah (Lestari, 2022). Selain kemudahan, aspek keamanan dalam mobile banking menjadi prioritas utama yang harus diperhatikan oleh bank.

Penggunaan teknologi biometrik hadir sebagai solusi inovatif dalam meningkatkan keamanan sistem perbankan. Teknologi biometrik memanfaatkan karakteristik biologis unik seseorang seperti sidik jari, wajah, suara, atau iris mata sebagai alat autentikasi identitas nasabah (Hartono et al., 2022). Sistem biometrik memiliki keunggulan karena sulit dipalsukan, tidak dapat ditiru, dan lebih akurat dibandingkan penggunaan PIN atau *password*. Namun, penerapan biometrik juga memiliki tantangan, terutama terkait perlindungan privasi data pribadi serta keamanan data dari risiko kebocoran atau penyalahgunaan. Oleh karena itu, penerapan biometrik harus disertai dengan regulasi yang jelas serta perlindungan hukum. Di Indonesia,

perlindungan teknologi digital diatur melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta peraturan Otoritas Jasa Keuangan dan Bank Indonesia guna memastikan penggunaan biometrik berjalan secara aman dan legal (Tarmizi, 2024). Selain isu privasi, tantangan lain dalam penerapan biometrik dalam mobile banking adalah kerentanan terhadap serangan siber seperti *data breach*, *spoofing*, dan *man-in-the-middle attack*. Kejahatan siber di sektor perbankan meningkat seiring meningkatnya pengguna layanan digital banking. Berdasarkan data Bank Indonesia, terdapat peningkatan kasus kejahatan digital sebesar 32% pada tahun 2023, terutama pada layanan mobile banking dan dompet digital (Bank Indonesia, 2023). Hal ini menunjukkan bahwa meskipun biometrik mampu memperkuat autentikasi, tetap diperlukan sistem keamanan berlapis seperti enkripsi data, *firewall*, serta *behavioral analytics* untuk mendeteksi aktivitas mencurigakan (Rahman & Purwanto, 2022).

Pada praktiknya, bank syariah di Indonesia seperti Bank Syariah Indonesia (BSI) telah mengintegrasikan sistem biometrik berupa *fingerprint* dan *face recognition* dalam aplikasi BSI Mobile untuk login dan otorisasi transaksi. Sistem ini dinilai lebih cepat, praktis, dan aman dibandingkan penggunaan PIN atau *password* saja (Wulandari & Hidayat, 2023). Namun, efektivitas biometrik juga ditentukan oleh kondisi perangkat pengguna, kualitas kamera, sensor sidik jari, serta kestabilan jaringan internet. Jika perangkat mengalami kerusakan pada sensor atau kualitas kamera rendah, verifikasi biometrik dapat gagal sehingga menghambat akses layanan mobile banking (Lestari & Saputra, 2022). Dari perspektif syariah, penggunaan biometrik dinilai tidak bertentangan dengan prinsip Islam karena termasuk dalam upaya menjaga *hifz al-mal* (perlindungan terhadap harta). Selama data biometrik yang dikumpulkan digunakan untuk tujuan kebaikan, tidak disalahgunakan, dan tidak melanggar privasi, maka hukumnya diperbolehkan (*mubah*) bahkan bisa menjadi *wajib* jika digunakan untuk mencegah kejahatan dan kemudaratan (Fatwa DSN-MUI No. 116 Tahun 2017). Ini menunjukkan bahwa integrasi teknologi dalam perbankan syariah harus tetap selaras dengan maqashid syariah yakni menjaga agama (*hifdz ad-din*), jiwa (*hifdz an-nafs*), akal (*hifdz al-aql*), keturunan (*hifdz an-nasl*), dan harta (*hifdz al-mal*) (Hidayatullah, 2021).

Dari sudut hukum positif, perlindungan data biometrik nasabah juga diatur dalam Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022). Data biometrik dikategorikan sebagai data pribadi spesifik, sehingga bank wajib mendapatkan persetujuan dari nasabah sebelum memproses, menyimpan, atau membagikannya kepada pihak lain (Kementerian Kominfo, 2023). Bank juga harus menerapkan prinsip transparansi, akuntabilitas, dan keamanan informasi dalam pengelolaan data untuk menghindari pelanggaran hukum. Jika ditinjau dari sisi manfaat, teknologi biometrik memiliki beberapa keunggulan penting dalam mobile banking, antara lain:

- 1) Keamanan tinggi, karena biometrik sulit dipalsukan dibandingkan PIN atau *password*.
- 2) Efisiensi waktu, proses login dan verifikasi transaksi lebih cepat (di bawah 3 detik).
- 3) Mengurangi risiko human error, seperti lupa *password* atau kehilangan kartu ATM.
- 4) Mendukung inklusi keuangan digital, terutama pada generasi muda yang akrab dengan teknologi (Putri & Arifin, 2023).

Namun, kelemahan biometrik tetap perlu diperhatikan, seperti:

- 1) Risiko penyalahgunaan data jika sistem diretas;

- 2) Ketergantungan pada teknologi perangkat (*device dependency*);
- 3) Tidak selalu efektif pada lansia atau pekerja fisik yang sidik jarinya menipis;
- 4) Isu etika ketika data wajah disimpan secara massal oleh server pusat perbankan (Basri & Hanafiah, 2021).

Dalam konteks pengembangan ke depan, *solusi hybrid* dianggap lebih ideal, yaitu menggabungkan biometrik dengan teknologi lain seperti *One Time Password (OTP)*, *Behavioral Biometrics* (pola mengetik, cara menggulir layar), *AI Fraud Detection*, dan *blockchain* untuk menjamin kerahasiaan data transaksi (Tarmizi, 2024). Solusi ini memungkinkan sistem keamanan mobile banking lebih adaptif dan responsif terhadap ancaman siber yang semakin kompleks. Selain itu, Bank Indonesia dan pemerintah juga terus memperkuat sistem keamanan perbankan digital melalui peningkatan enkripsi data, penggunaan firewall, pemantauan aktivitas mencurigakan (*fraud detection*), serta regulasi perlindungan data konsumen. Upaya ini dilakukan untuk meningkatkan kepercayaan nasabah terhadap sistem perbankan digital, khususnya mobile banking yang menggunakan biometrik dalam proses verifikasi (Adinugraha & Sartika, 2020). Dengan demikian, dapat disimpulkan bahwa teknologi biometrik memberikan dampak positif dalam peningkatan keamanan verifikasi mobile banking bank syariah. Namun, implementasinya tetap harus diimbangi dengan perlindungan hukum, edukasi nasabah, serta kesiapan infrastruktur teknologi agar sistem ini dapat digunakan secara efektif dan terpercaya.

## KESIMPULAN

Bahwa perkembangan teknologi berbanding lurus dengan perkembangan gaya hidup saat ini. Seiring dengan semakin banyaknya informasi yang tersedia melalui berbagai media, baik cetak maupun elektronik, gaya hidup masyarakat saat ini yang terus berkembang memerlukan akses informasi yang cepat untuk memenuhi kebutuhan informasinya. Karena kebutuhan akan mobilitas dan akses terhadap informasi, gaya hidup masyarakat sangat erat kaitannya dengan perangkat teknologi saat ini. Dapat di simpulkan bahwa Perkembangan teknologi berbanding lurus dengan perkembangan gaya hidup saat ini. Seiring dengan semakin banyaknya informasi yang tersedia melalui berbagai media, baik cetak maupun elektronik, gaya hidup masyarakat saat ini yang terus berkembang memerlukan akses informasi yang cepat untuk memenuhi kebutuhan informasinya. Karena kebutuhan akan mobilitas dan akses terhadap informasi, gaya hidup masyarakat sangat erat kaitannya dengan perangkat teknologi saat ini.

## DAFTAR PUSTAKA

- Adinugraha, F., & Sartika, D. (2020). Pemanfaatan Teknologi Digital dalam Layanan Perbankan Syariah di Indonesia. *Jurnal Ekonomi Syariah*, 12(2), 145–158. <https://doi.org/10.36908/jes.v12i2.124>
- Arikunto, S. (2013). *Prosedur Penelitian: Suatu Pendekatan Praktik*. Rineka Cipta.
- Bank Indonesia. (2023). *Laporan Profil Risiko Keuangan Digital di Indonesia*. Bank Indonesia. <https://www.bi.go.id/id/publikasi>
- Basri, S., & Hanafiah, H. (2021). Etika Pengelolaan Data Biometrik dalam Sistem Keuangan Digital. *Jurnal Teknologi Informasi*, 7(3), 201–212. <https://doi.org/10.32528/jti.v7i3.5342>
- Budhi Hardjo. (2021). Keamanan Informasi Digital dalam Sistem Pembayaran. *Jurnal Sistem Informasi*, 6(1), 34–48.

- Fachmi, M., & Setiawan, A. (2020). Pengaruh Teknologi Informasi terhadap Perubahan Gaya Hidup Masyarakat Digital. *Journal of Social and Technology*, 4(1), 56–66. <https://doi.org/10.22219/jst.v4i1.9812>
- Firjatullah, A., Rahman, B., & Setyoko, H. (2021). Electronic Banking dan Inovasi Layanan Perbankan Digital. *Jurnal Ilmu Ekonomi*, 13(1), 77–85. <https://doi.org/10.21776/ub.jie.2021.013>
- Hartono, B., Rizaldy, M., & Lestari, Y. (2022). Implementasi Biometrik pada Sistem Pembayaran Digital. *Jurnal Informatika*, 9(2), 112–123. <https://doi.org/10.23917/informatika.v9i2.5634>
- Hidayatullah, I. (2021). Biometrik dalam Perspektif Maqashid Syariah dan Perlindungan Data. *Jurnal Ilmiah Ekonomi Syariah*, 5(4), 255–268. <https://doi.org/10.24235/jies.v5i4.6248>
- Kementerian Kominfo. (2023). Pedoman Perlindungan Data Biometrik dan Privasi Digital Nasabah. Kominfo RI. <https://www.kominfo.go.id>
- Kusuma, H. (2023). Teknologi Biometrik dan Perannya dalam Sistem Keamanan Perbankan Digital. *Jurnal Teknik Informatika*, 10(1), 45–58. <https://doi.org/10.3390/jti.v10i1.1043>
- Lestari, A. (2022). Mobile Banking Syariah dan Prinsip Kepatuhan Syariah. *Jurnal Ekonomi Syariah dan Teknologi Finansial*, 4(3), 178–189.
- Lestari, A., & Saputra, R. (2022). Analisis Kesiapan Infrastruktur Biometrik pada Aplikasi Mobile Banking. *Jurnal Teknologi Informasi*, 7(2), 121–130. <https://doi.org/10.15294/jti.v7i2.7342>
- Nurdin, I., Ahmad, S., & Latifah, M. (2021). Pemanfaatan Mobile Banking dalam Layanan Perbankan Syariah. *Jurnal Manajemen dan Bisnis*, 5(2), 88–97. <https://doi.org/10.21009/jmb.v5i2.313>
- OJK. (2023). Laporan Kejahatan Siber di Sektor Jasa Keuangan 2023. Otoritas Jasa Keuangan. <https://www.ojk.go.id>
- Putra, A., Rahim, A., & Firmansyah, M. (2023). Tren Penggunaan Digital Banking di Indonesia Pasca Pandemi. *Jurnal Perbankan dan Keuangan*, 8(1), 22–38. <https://doi.org/10.47312/jpk.v8i1.9083>
- Putri, V., & Arifin, D. (2023). Preferensi Generasi Milenial terhadap Teknologi Keuangan Digital. *Jurnal Manajemen dan Teknologi Finansial*, 9(2), 76–88.
- Putri, V., & Fahrozi, M. (2021). Analisis Autentikasi PIN dan OTP pada Sistem Pembayaran Digital. *Jurnal Komputer dan Sistem Informasi*, 3(2), 44–52. <https://doi.org/10.30812/jksi.v3i2.674>
- Rahman, A., & Purwanto, D. (2022). Ancaman Siber terhadap Sistem Keamanan Biometrik pada Mobile Banking. *Jurnal Cyber Security*, 11(2), 109–122. <https://doi.org/10.23919/jcs.v11i2.8451>
- Saputri, L., Hasanah, E., & Mulyani. (2023). Digital Banking dan Perilaku Generasi Z. *Jurnal Ekonomi Digital*, 5(2), 143–155. <https://doi.org/10.1016/j.jed.2023.02.005>
- Sugiyono. (2019). *Metode Penelitian Kualitatif, Kuantitatif, dan R&D*. Alfabeta.
- Tarmizi, A. (2024). Hybrid Security pada Sistem Autentikasi Mobile Banking. *Journal of Digital Security*, 12(1), 34–49. <https://doi.org/10.14421/jds.v12i1.6541>
- Wulandari, S., & Hidayat, R. (2023). Penerapan Face Recognition pada BSI Mobile Banking. *Jurnal Teknologi Perbankan*, 6(1), 88–97. <https://doi.org/10.25777/jtp.v6i1.5934>
- Zed, M. (2014). *Metode Penelitian Kepustakaan*. Yayasan Obor Indonesia.