Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi
Vol. 3, No. 1, September 2024, pp. 81−89
E-ISSN: 2963-4148 | P-ISSN: 2963-4423, DOI:10.33050

Pentingnya Edukasi dalam Mengatasi Keamanan Data Mobile Banking di Indonesia

Dwi Cahyono[1*], Rifqi Fahrudin[2], Alwiyah[3], Amelia Sinclair[4]
[1] Fakultas Teknik Informatika, Universitas Dr.Soetomo, Surabaya, Indonesia
[2] Fakultas Sistem Informasi, Universitas Catur Insan Cendekia, Jawa Barat, Indonesia
[3] Fakultas Ekonomi dan Bisnis, Universitas Muhammadiyah Semarang, Jawa Tengah, Indonesia
[4] Fakultas Sistem informasi, EESP Incorporation, Samudra Hindia Britania
[1]dwikk@unitomo.ac.id, [2]rifqi.fahrudin@cic.ac.id, [3]alwiyahmahdaly@yahoo.com, [4] sinclairrr@eesp.io
***Corresponding Author**

Article Info

Article history:

Penyerahan Agustus 04, 2024
Revisi September 12, 2024
Diterima September 21, 2024
Diterbitkan September 23, 2024

Kata Kunci:

Keamanan Data
Mobile Banking
Enkripsi
Autentikasi Multifactor
Edukasi Pengguna

ABSTRACT

Keamanan data dalam aplikasi *mobile banking* menjadi isu yang semakin krusial di tengah pesatnya adopsi layanan perbankan digital di Indonesia. Selain tantangan teknologi, edukasi pengguna menjadi salah satu faktor penting dalam menjaga keamanan data. Artikel ini mengidentifikasi tantangan keamanan data dan menyoroti pentingnya peningkatan kesadaran serta edukasi pengguna *mobile banking* di Indonesia. Penelitian ini menggunakan pendekatan deskriptif kualitatif melalui survei terhadap 200 pengguna dan wawancara mendalam dengan 10 pakar keamanan dari bank-bank besar di Indonesia. Fokus penelitian ini juga pada pentingnya pelatihan dan pendidikan bagi pengguna dan staf perbankan terkait praktik keamanan yang baik, termasuk enkripsi *end-to-end*, autentikasi multifaktor, dan teknologi biometrik. Hasil menunjukkan bahwa 65% pengguna pernah menghadapi serangan *phishing* dan 50% khawatir terhadap *malware*, dengan kesadaran akan keamanan masih rendah. Artikel ini menekankan bahwa peningkatan kesadaran dan edukasi merupakan langkah penting untuk menciptakan lingkungan perbankan digital yang lebih aman dan terpercaya. Rekomendasi praktis diberikan untuk bank agar berinvestasi dalam program edukasi yang berkelanjutan untuk melindungi pengguna dari ancaman keamanan siber.

Data security in mobile banking applications is becoming an increasingly crucial issue amidst the rapid adoption of digital banking services in Indonesia. In addition to technological challenges, user education is one of the important factors in maintaining data security. This article identifies data security challenges and highlights the importance of increasing awareness and education of mobile banking users in Indonesia. This study uses a qualitative descriptive approach through a survey of 200 users and in-depth interviews with 10 security experts from major banks in Indonesia. The focus of this study also focuses on the importance of training and education for users and banking staff on good security practices, including end-to-end encryption, multifactor authentication, and biometric technology. The results show that 65% of users have experienced phishing attacks and 50% are concerned about malware, with security awareness still low. This article emphasizes that increasing awareness and education are important steps to create a safer and more trusted digital banking environment. Practical recommendations are provided for banks to invest in ongoing education programs to protect users from cybersecurity threats.

This is an open access article under the CC BY license.

*Corresponding Author:
Dwi Cahyono (dwikk@unitomo.ac.id)
DOI: https://doi.org/10.33050/mentari.v3i1
This is an open-access article under the CC-BY license (https://creativecommons.org/licenses/by/4.0/
©Authors retain all copyrights

1. PENDAHULUAN

Dalam beberapa tahun terakhir, penggunaan *mobile banking* di Indonesia telah mengalami peningkatan yang signifikan. Hal ini didorong oleh kemajuan teknologi informasi dan komunikasi, serta peningkatan penetrasi smartphone di kalangan masyarakat. *mobile banking* menawarkan berbagai kemudahan, seperti akses perbankan yang cepat dan efisien, transaksi yang dapat dilakukan kapan saja dan di mana saja, serta fitur-fitur yang mendukung kebutuhan finansial pengguna [1]. Berdasarkan data dari Bank Indonesia, jumlah pengguna *mobile banking* meningkat lebih dari dua kali lipat dalam lima tahun terakhir, menunjukkan adaptasi yang cepat terhadap teknologi ini [2]. Namun, seiring dengan peningkatan penggunaan *mobile banking*, isu keamanan data menjadi semakin krusial [3]. Keamanan data mencakup berbagai aspek, mulai dari perlindungan terhadap akses tidak sah, pencegahan penipuan, hingga perlindungan terhadap pencurian identitas. Dalam konteks *mobile banking*, keamanan data bukan hanya tanggung jawab penyedia layanan, tetapi juga pengguna [4]. Kesadaran dan pemahaman tentang pentingnya menjaga keamanan data sangat penting untuk mencegah potensi risiko yang dapat merugikan kedua belah pihak [5].

Meskipun telah banyak penelitian dilakukan terkait keamanan data dalam *mobile banking*, terdapat beberapa gap yang belum sepenuhnya terisi dalam literatur yang ada. Sebagian besar penelitian tentang keamanan *mobile banking* dilakukan dalam konteks negara-negara maju, sementara studi yang berfokus pada Indonesia masih terbatas [6], [7]. Kondisi teknologi, regulasi, dan perilaku pengguna di Indonesia mungkin berbeda, sehingga penelitian lokal sangat diperlukan. Selain itu, kesadaran dan edukasi pengguna tentang keamanan data juga menjadi aspek penting yang seringkali diabaikan. Banyak penelitian lebih menekankan pada aspek teknis dari keamanan data, seperti enkripsi dan *firmwall*, namun kurang membahas peran dan kesadaran pengguna dalam menjaga keamanan data [8]. Dalam konteks ini, edukasi yang lebih mendalam tentang praktik keamanan perlu diperkuat, baik bagi pengguna maupun staf perbankan. Studi-studi yang ada seringkali hanya menyarankan solusi tanpa mengevaluasi efektivitasnya secara empiris dalam konteks nyata. Adopsi teknologi keamanan baru seperti biometrik dan kecerdasan buatan dalam *mobile banking* di Indonesia juga belum banyak diteliti [9], [10].

Meskipun telah banyak upaya dilakukan untuk meningkatkan keamanan data dalam aplikasi *mobile banking*, masih terdapat sejumlah masalah yang perlu diidentifikasi dan diatasi [1]. Beberapa masalah utama yang terkait dengan keamanan data pada aplikasi *mobile banking* di Indonesia antara lain: peningkatan serangan siber yang menargetkan aplikasi *mobile banking*, termasuk *phishing*, *malware*, dan *hacking*, Rendahnya tingkat kesadaran pengguna tentang praktik keamanan yang baik, seperti penggunaan kata sandi yang kuat dan berhati-hati terhadap tautan mencurigakan, beberapa bank mungkin masih menggunakan teknologi keamanan yang usang atau kurang optimal dalam menghadapi ancaman baru, serta keterbatasan dalam kebijakan dan regulasi yang mengatur keamanan data pada aplikasi *mobile banking*, yang mungkin belum sepenuhnya memadai untuk menghadapi ancaman yang berkembang[11], [12]. Oleh karena itu, edukasi kepada pengguna terkait keamanan siber sangat dibutuhkan untuk mengurangi risiko yang dihadapi baik oleh pengguna maupun pihak perbankan.

Tujuan utama dari penelitian ini adalah untuk mengidentifikasi tantangan-tantangan utama yang terkait dengan keamanan data dalam penggunaan aplikasi *mobile banking* di Indonesia, dengan fokus pada peran edukasi dan pelatihan pengguna dalam menghadapi ancaman keamanan. Secara spesifik, penelitian ini bertujuan untuk mengidentifikasi berbagai tantangan yang dihadapi oleh pengguna dan penyedia layanan *mobile banking* terkait keamanan data, menganalisis solusi-solusi yang telah diterapkan oleh bank-bank di Indonesia dan efektivitasnya dalam meningkatkan keamanan data, serta mengusulkan rekomendasi yang dapat diadopsi oleh bank dan penyedia layanan *mobile banking* untuk meningkatkan keamanan data melalui program edukasi dan pelatihan yang berkelanjutan.

Penelitian ini memiliki beberapa aspek originalitas yang membedakannya dari penelitian sebelumnya. Pertama, penelitian ini secara khusus difokuskan pada konteks Indonesia, yang memiliki karakteristik

unik dalam hal penggunaan *mobile banking* dan tantangan keamanannya. Kedua, penelitian ini tidak hanya mengidentifikasi tantangan teknis tetapi juga mempertimbangkan aspek edukasi pengguna dan regulasi yang relevan. Ketiga, penelitian ini akan melakukan evaluasi empiris terhadap solusi-solusi keamanan yang telah diterapkan, memberikan wawasan tentang efektivitas dan area yang perlu ditingkatkan. Keempat, penelitian ini akan mengeksplorasi potensi adopsi teknologi keamanan terbaru, seperti biometrik dan kecerdasan buatan, dalam meningkatkan keamanan data pada aplikasi *mobile banking* di Indonesia. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi signifikan baik dari segi teori maupun praktik, membantu meningkatkan keamanan data dalam penggunaan *mobile banking* di Indonesia, serta meningkatkan kesadaran pengguna melalui edukasi yang efektif.

1.1. Tinjauan Pustaka

Keamanan data dalam *mobile banking* mencakup berbagai definisi dan konsep dasar yang esensial untuk dipahami. Keamanan data pada aplikasi *mobile banking* melibatkan perlindungan informasi sensitif pengguna dari akses yang tidak sah, manipulasi, dan pencurian [13], [14]. Konsep dasar ini mencakup mekanisme enkripsi untuk menjaga kerahasiaan data, autentikasi untuk memastikan identitas pengguna, dan otorisasi untuk memastikan bahwa hanya pihak yang berwenang yang dapat mengakses data tertentu [15]. Selain itu, keamanan data juga mencakup perlindungan terhadap serangan siber seperti *phishing*, *malware*, dan *hacking*, yang dapat membahayakan integritas dan ketersediaan data pengguna [16], [17]. Perlindungan ini tidak hanya tergantung pada teknologi yang digunakan, tetapi juga pada edukasi pengguna dan pelatihan staf bank mengenai praktik terbaik dalam keamanan digital [18]. Penerapan kebijakan keamanan yang ketat oleh penyedia layanan *mobile banking* sangat penting untuk menciptakan lingkungan perbankan yang aman dan terpercaya bagi pengguna.

Tantangan keamanan data dalam *mobile banking* telah menjadi fokus banyak penelitian di bidang ini. Beberapa tantangan utama yang dihadapi meliputi peningkatan jumlah serangan siber yang semakin canggih dan beragam. Serangan seperti *phishing*, di mana penyerang mencoba memperoleh informasi sensitif dengan menyamar sebagai entitas terpercaya, dan *malware*, yang dapat menginfeksi perangkat pengguna dan mencuri data, merupakan ancaman nyata yang harus dihadapi [2]. Selain aspek teknis, rendahnya tingkat kesadaran pengguna mengenai praktik keamanan yang baik, seperti penggunaan kata sandi yang kuat dan berhati-hati dalam mengklik tautan mencurigakan, menggarisbawahi pentingnya edukasi yang efektif. Edukasi pengguna mengenai risiko dan cara mencegah serangan siber sangat penting dalam mengurangi kerentanan terhadap ancaman ini [19]. Di sisi lain, beberapa bank mungkin masih menggunakan sistem keamanan yang usang atau kurang optimal, serta kebijakan dan regulasi yang belum sepenuhnya memadai, juga merupakan tantangan yang perlu diatasi untuk meningkatkan keamanan data dalam *mobile banking* [20].

Untuk mengatasi tantangan-tantangan tersebut, berbagai solusi keamanan data telah diimplementasikan dan ditinjau dalam literatur. Solusi teknis seperti penggunaan enkripsi *end-to-end* memastikan bahwa data yang dikirimkan antara pengguna dan bank tidak dapat dibaca oleh pihak ketiga. Implementasi autentikasi multifaktor, yang memerlukan lebih dari satu metode verifikasi identitas, juga telah terbukti efektif dalam meningkatkan keamanan [21]. Selain itu, adopsi teknologi baru seperti biometrik, yang menggunakan pengenalan sidik jari atau wajah untuk autentikasi, telah menambah lapisan keamanan tambahan [22]. Namun, implementasi solusi teknis ini harus dibarengi dengan program edukasi yang tepat sasaran bagi pengguna *mobile banking*, yang seringkali kurang menyadari risiko yang dihadapi. Beberapa bank telah meluncurkan kampanye edukasi untuk meningkatkan kesadaran pengguna mengenai praktik keamanan yang baik, seperti mengenali email *phishing* atau pentingnya memperbarui kata sandi secara rutin [23]. Pelatihan berkelanjutan bagi staf perbankan juga sangat diperlukan untuk menghadapi ancaman keamanan yang terus berkembang [24]. Evaluasi dan peningkatan berkelanjutan terhadap kebijakan dan regulasi keamanan data juga diperlukan untuk memastikan bahwa mereka tetap relevan dan efektif dalam menghadapi ancaman yang berkembang [25].

2. METODOLOGI PENELITIAN

2.1. Desain Penelitian

Desain Penelitian Penelitian ini menggunakan pendekatan deskriptif kualitatif untuk memahami tantangan dan solusi keamanan data dalam penggunaan aplikasi *mobile banking* di Indonesia. Pendekatan ini dipilih karena memungkinkan peneliti untuk menggali secara mendalam persepsi, pengalaman, dan pandangan para pengguna serta pihak terkait dalam industri perbankan. Data dikumpulkan melalui berbagai sumber, termasuk

survei dan wawancara, untuk mendapatkan pemahaman yang komprehensif mengenai isu yang sedang diteliti [26].

2.2. Sampel dan Teknik Pengambilan Sampel

Populasi dalam penelitian ini meliputi pengguna aplikasi *mobile banking* dan pihak terkait dalam industri perbankan di Indonesia [27], [28]. Sampel dipilih menggunakan teknik purposive sampling, di mana peneliti memilih responden yang dianggap memiliki pengetahuan dan pengalaman yang relevan dengan topik penelitian. Pemilihan responden juga mempertimbangkan pengguna yang telah menggunakan aplikasi *mobile banking* selama lebih dari satu tahun dan memiliki pengalaman terkait masalah keamanan data. Hal ini dilakukan untuk mendapatkan informasi yang lebih mendalam terkait kesadaran dan edukasi pengguna terhadap praktik keamanan dalam *mobile banking* [29]. Sebanyak 200 pengguna *mobile banking* dari berbagai latar belakang serta beberapa pakar keamanan data dari bank-bank besar di Indonesia dijadikan sampel untuk mendapatkan informasi yang bervariasi dan mendalam, sebagaimana ditunjukkan dalam Tabel 1.

Tabel 1. Komposisi Sampel

Kategori	Jumlah Responden
Pengguna *mobile banking*	200
Pakar Keamanan Data	10
Total	210

Tabel 1 menunjukkan bahwa komposisi sampel terdiri dari pengguna aplikasi *mobile banking* sebagai fokus utama, serta pakar keamanan data yang memberikan wawasan mendalam terkait kebijakan dan praktik keamanan yang telah diterapkan di perbankan. Sampel ini dipilih untuk mewakili berbagai perspektif yang relevan dalam meneliti tantangan dan solusi keamanan data dalam aplikasi *mobile banking* di Indonesia.

2.3. Instrumen Penelitian

Untuk mengumpulkan data, penelitian ini menggunakan beberapa instrumen, yaitu survei dan wawancara mendalam. Survei disebarkan kepada pengguna aplikasi *mobile banking* untuk mengumpulkan data kuantitatif mengenai tantangan yang mereka hadapi dan solusi yang mereka anggap efektif [30]. Survei ini juga menilai tingkat kesadaran dan pemahaman pengguna terhadap praktik keamanan data yang telah diterapkan oleh bank, serta program edukasi yang mereka terima terkait keamanan siber. Selain itu, wawancara mendalam dilakukan dengan pakar keamanan data dari bank-bank besar di Indonesia untuk mendapatkan wawasan kualitatif yang lebih rinci dan mendalam mengenai isu yang sedang diteliti. Wawancara ini juga mencakup pertanyaan terkait kebijakan edukasi yang diterapkan bank dalam meningkatkan kesadaran pengguna mengenai ancaman keamanan siber.

2.4. Prosedur Pengumpulan Data

Pengumpulan data dilakukan dalam beberapa tahap. Pertama, survei disebarkan secara online kepada pengguna *mobile banking* yang telah dipilih sebagai sampel. Responden diberikan waktu dua minggu untuk mengisi survei tersebut. Survei ini juga mengukur apakah pengguna telah menerima edukasi dari bank mengenai praktik keamanan data. Kedua, wawancara mendalam dilakukan dengan pakar keamanan data melalui platform video conference untuk mematuhi protokol kesehatan. Setiap wawancara direkam dan ditranskripsikan untuk dianalisis lebih lanjut. Seluruh data yang dikumpulkan kemudian dikompilasi dan disimpan dengan aman untuk analisis selanjutnya. Data terkait pengalaman dan pandangan para pakar mengenai pentingnya edukasi dan kesadaran dalam menghadapi ancaman siber juga dikumpulkan selama wawancara.

2.5. Teknik Analisis Data

Data yang dikumpulkan dianalisis menggunakan metode analisis deskriptif. Data kuantitatif dari survei dianalisis menggunakan statistik deskriptif untuk mengidentifikasi pola dan tren umum terkait tantangan dan solusi keamanan data dalam *mobile banking*. Analisis ini juga melibatkan evaluasi program edukasi yang telah diterima oleh pengguna dan efektivitasnya dalam meningkatkan kesadaran keamanan. Sementara itu, data kualitatif dari wawancara dianalisis menggunakan analisis tematik untuk mengidentifikasi tema-tema kunci dan wawasan mendalam mengenai isu yang diteliti. Kombinasi analisis kuantitatif dan kualitatif ini

diharapkan dapat memberikan gambaran yang komprehensif dan mendalam mengenai tantangan dan solusi keamanan data dalam penggunaan aplikasi *mobile banking* di Indonesia, serta menilai dampak dari edukasi yang diberikan oleh bank terhadap peningkatan kesadaran pengguna [31], [32].

3. HASIL DAN PEMBAHASAN

3.1. Identifikasi Tantangan Keamanan Data

Berdasarkan data yang dikumpulkan dari survei dan wawancara mendalam, berbagai tantangan yang dihadapi dalam menjaga keamanan data di aplikasi *mobile banking* di Indonesia telah diidentifikasi. Dari 200 pengguna *mobile banking* yang disurvei, sebanyak 65% mengaku pernah mengalami atau mengetahui kasus *phishing*, di mana penyerang mencoba memperoleh informasi sensitif dengan menyamar sebagai entitas terpercaya. Sebanyak 50% responden melaporkan bahwa mereka khawatir terhadap ancaman *malware* yang dapat menginfeksi perangkat mereka dan mencuri data. Tingkat kesadaran pengguna yang rendah mengenai pentingnya praktik keamanan digital menjadi salah satu tantangan paling mendasar. Sebanyak 40% responden mengakui bahwa mereka tidak selalu menggunakan kata sandi yang kuat atau menggantinya secara berkala, yang menunjukkan pentingnya edukasi berkelanjutan untuk meningkatkan kesadaran dan pemahaman pengguna. Selain itu, wawancara dengan pakar keamanan data dari bank-bank besar di Indonesia mengungkapkan bahwa beberapa bank masih menggunakan teknologi keamanan yang usang, yang kurang optimal dalam menghadapi ancaman baru yang terus berkembang. Tantangan-tantangan ini menjadi lebih kompleks karena kurangnya pelatihan dan edukasi yang diberikan kepada pengguna mengenai keamanan siber [33].

Sebagai gambaran lebih rinci, Tabel 2 merangkum tantangan keamanan utama yang dihadapi oleh pengguna *mobile banking* di Indonesia.

Tabel 2. Tantangan Keamanan Data dalam *mobile banking*

Tantangan Keamanan	**Persentase Responden Mengalami (%)**
phishing	65
malware	50
Rendahnya Kesadaran Pengguna	40
Penggunaan Teknologi Keamanan Usang	0

Tabel 2 menunjukkan bahwa masalah keamanan seperti *phishing* dan *malware* merupakan ancaman yang signifikan bagi pengguna aplikasi *mobile banking*. Rendahnya tingkat kesadaran pengguna terhadap praktik keamanan yang baik menggarisbawahi pentingnya program edukasi yang sistematis dan berkelanjutan untuk meningkatkan pemahaman tentang risiko digital.

3.2. Analisis Solusi Keamanan Data

Berbagai solusi keamanan data telah diimplementasikan oleh bank-bank di Indonesia untuk mengatasi tantangan tersebut. Dari hasil survei, sebanyak 70% pengguna menyatakan bahwa bank mereka telah menggunakan enkripsi *end-to-end* untuk melindungi data mereka. Solusi ini dianggap efektif oleh 80% responden, yang merasa lebih aman saat menggunakan aplikasi *mobile banking*. Autentikasi multifaktor juga telah diadopsi oleh banyak bank, dengan 60% responden melaporkan bahwa mereka menggunakan metode ini untuk masuk ke akun mereka. Teknologi biometrik, seperti pengenalan sidik jari dan wajah, mulai banyak diterapkan, meskipun adopsinya masih relatif baru.

Namun, meskipun solusi teknis ini sudah mulai diterapkan, wawancara dengan pakar keamanan mengungkapkan bahwa kampanye edukasi pengguna mengenai praktik keamanan yang baik masih belum optimal, sebagaimana tercermin dari nol persen responden yang melaporkan telah menerima pelatihan terkait keamanan dari bank mereka. Padahal, edukasi memainkan peran penting dalam membentuk kesadaran pengguna mengenai ancaman keamanan yang dapat dihadapi dalam aktivitas digital sehari-hari. Bank perlu melengkapi solusi teknis dengan kampanye edukasi pengguna yang lebih efektif untuk menciptakan perlindungan komprehensif.

Tabel 3 merangkum solusi keamanan yang telah diimplementasikan oleh bank-bank di Indonesia beserta efektivitasnya.

Tabel 3. Solusi Keamanan Data yang Diimplementasikan

Solusi Keamanan	Persentase Implementasi (%)	Persentase Efektivitas (%)
Enkripsi *end-to-end*	70	80
Autentikasi Multifaktor	60	75
Teknologi Biometrik	40	85
Kampanye Edukasi Pengguna	0	0

Tabel 3 menunjukkan bahwa meskipun solusi teknis seperti enkripsi *end-to-end* dan autentikasi multifaktor sudah banyak diterapkan, efektivitas program edukasi pengguna masih sangat minim. Hal ini menunjukkan bahwa terdapat gap yang signifikan dalam upaya meningkatkan kesadaran keamanan digital di kalangan pengguna *mobile banking*, yang memerlukan perhatian lebih dari lembaga perbankan. Bank di Indonesia harus mempertimbangkan strategi edukasi yang terstruktur, seperti kampanye kesadaran keamanan digital, pelatihan daring, dan tutorial interaktif yang secara efektif dapat meningkatkan perilaku keamanan di kalangan pengguna mereka [34].

3.3. Diskusi

Hasil penelitian ini menunjukkan bahwa tantangan keamanan data dalam aplikasi *mobile banking* di Indonesia sangat kompleks dan beragam. Temuan ini konsisten dengan literatur yang ada, yang menyatakan bahwa serangan siber seperti *phishing* dan *malware* merupakan ancaman utama dalam sektor perbankan digital. Rendahnya kesadaran pengguna tentang praktik keamanan juga telah diidentifikasi sebagai masalah signifikan dalam penelitian sebelumnya. Penelitian ini memperkuat argumen bahwa tingkat kesadaran pengguna yang rendah memerlukan intervensi edukasi yang lebih terstruktur untuk mencegah kerentanan terhadap serangan siber.

Solusi-solusi yang telah diimplementasikan, seperti enkripsi *end-to-end* dan autentikasi multifaktor, terbukti efektif dalam meningkatkan keamanan, sebagaimana didukung oleh literatur yang menyarankan penggunaan teknologi ini sebagai langkah penting dalam mitigasi risiko. Namun, temuan ini juga menunjukkan bahwa solusi teknis saja tidak cukup. Edukasi berkelanjutan bagi pengguna tentang praktik keamanan digital, seperti pentingnya menggunakan kata sandi yang kuat dan berhati-hati terhadap tautan mencurigakan, harus menjadi bagian integral dari strategi keamanan perbankan. Meskipun artikel ini menggunakan statistik deskriptif untuk menganalisis tantangan dan solusi, analisis kuantitatif yang lebih mendalam dapat memperkuat argumen dengan menyajikan korelasi yang lebih jelas antara tingkat edukasi dan kesadaran pengguna dengan efektivitas solusi keamanan yang diterapkan.

Adopsi teknologi biometrik, meskipun masih dalam tahap awal, menunjukkan potensi besar dalam meningkatkan keamanan data. Teknologi ini, jika dikombinasikan dengan kampanye edukasi yang efektif, dapat membantu mengurangi risiko serangan siber secara signifikan. Kampanye edukasi pengguna memainkan peran yang sangat penting dalam meningkatkan kesadaran dan perilaku keamanan, sesuai dengan temuan dari studi lain yang menekankan pentingnya edukasi dalam pencegahan ancaman siber. Penelitian ini mendukung pandangan bahwa edukasi yang proaktif dan berkelanjutan merupakan kunci dalam membentuk perilaku pengguna yang lebih sadar akan keamanan.

Implikasi praktis dari penelitian ini menunjukkan bahwa bank harus terus berinvestasi dalam teknologi keamanan terbaru dan menjalankan program edukasi yang berkelanjutan untuk pengguna mereka. Bank harus mempertimbangkan untuk menggabungkan teknologi canggih dengan pelatihan praktis dan kampanye kesadaran yang efektif untuk menciptakan lingkungan perbankan digital yang lebih aman dan dapat dipercaya. Selain itu, kebijakan dan regulasi juga perlu diperbarui untuk mencakup ancaman dan solusi keamanan yang berkembang, memastikan bahwa perlindungan data tetap relevan dan efektif. Kebijakan ini harus didukung oleh program pelatihan berkala bagi karyawan bank agar mereka selalu siap menghadapi ancaman keamanan terbaru, serta upaya edukasi yang menargetkan pengguna dengan memberikan informasi yang mudah diakses tentang praktik keamanan terbaik.

4. KESIMPULAN

Penelitian ini mengungkap berbagai tantangan utama dalam menjaga keamanan data pada aplikasi *mobile banking* di Indonesia, termasuk serangan siber seperti *phishing* dan *malware*, rendahnya kesadaran pengguna mengenai praktik keamanan yang baik, serta penggunaan teknologi keamanan yang usang oleh beberapa bank. Temuan ini menggarisbawahi bahwa tantangan keamanan data tidak hanya bersifat teknis, tetapi juga terkait dengan aspek kesadaran dan edukasi pengguna. Hal ini menunjukkan pentingnya pendekatan yang lebih menyeluruh yang menggabungkan teknologi dan edukasi dalam upaya mitigasi risiko.

Solusi yang telah diidentifikasi dalam penelitian ini mencakup penggunaan enkripsi *end-to-end* dan autentikasi multifaktor, yang terbukti efektif dalam meningkatkan keamanan data. Adopsi teknologi biometrik, seperti pengenalan sidik jari dan wajah, meskipun masih dalam tahap awal, menunjukkan potensi besar dalam memberikan lapisan keamanan tambahan. Namun, efektivitas dari solusi teknis ini akan jauh lebih optimal jika didukung oleh kampanye edukasi yang menyeluruh bagi pengguna. Edukasi dan pelatihan yang efektif akan membantu meningkatkan kesadaran pengguna tentang pentingnya praktik keamanan, seperti penggunaan kata sandi yang kuat, penghindaran tautan mencurigakan, dan pemahaman akan risiko serangan siber.

Penelitian ini menekankan pentingnya bank dan penyedia layanan *mobile banking* untuk terus berinvestasi dalam teknologi keamanan terbaru, sekaligus mengintegrasikan program edukasi dan pelatihan berkelanjutan bagi pengguna mereka. Pengguna yang teredukasi dengan baik akan lebih mampu melindungi data mereka dari ancaman siber, yang pada akhirnya juga akan membantu mengurangi beban risiko bagi bank. Bank diharapkan tidak hanya mengandalkan teknologi keamanan, tetapi juga memprioritaskan kampanye edukasi yang proaktif untuk meningkatkan kesadaran dan perilaku keamanan pengguna.

Selain itu, kebijakan dan regulasi perlu diperbarui untuk mencakup ancaman dan solusi keamanan yang terus berkembang. Regulasi ini harus menyertakan ketentuan yang mewajibkan penyedia layanan perbankan digital untuk memberikan program edukasi yang komprehensif kepada pengguna dan staf mereka. Dengan demikian, penelitian ini memberikan kontribusi signifikan dalam memahami tantangan dan solusi keamanan data dalam aplikasi *mobile banking* di Indonesia, serta memberikan rekomendasi praktis yang dapat diadopsi untuk menciptakan lingkungan perbankan digital yang lebih aman dan terpercaya melalui pendekatan yang terintegrasi antara teknologi dan edukasi.

SARAN

Berdasarkan temuan penelitian ini, disarankan agar bank dan penyedia layanan *mobile banking* di Indonesia meningkatkan investasi dalam teknologi keamanan seperti enkripsi *end-to-end*, autentikasi multifaktor, dan biometrik. Investasi ini harus didukung oleh program edukasi yang berkelanjutan untuk meningkatkan kesadaran pengguna tentang risiko keamanan siber. Edukasi dapat dilakukan melalui kampanye kesadaran, tutorial online, dan pelatihan interaktif, yang disesuaikan dengan tingkat pemahaman pengguna. Selain itu, regulasi perlu diperbarui secara berkala untuk menyesuaikan dengan perkembangan teknologi dan ancaman baru, dengan memastikan lembaga keuangan memberikan edukasi komprehensif kepada pengguna dan staf. Kolaborasi antara bank, regulator, dan pengguna juga penting dalam menciptakan ekosistem *mobile banking* yang aman melalui berbagi informasi dan praktik terbaik dalam menjaga keamanan data.

UCAPAN TERIMAKASIH

Terima kasih kepada semua pihak yang telah membantu dan mendukung penelitian ini, khususnya para responden survei dan narasumber wawancara yang telah memberikan waktu dan informasi berharga. Terima kasih juga kepada semua rekan kerja yang memberikan dorongan dan bimbingan selama proses penelitian ini.

5. DEKLARASI

5.1. Kontribusi Penulis

Konseptualisasi: K.B.R.; Metodologi: L.K.C.; Perangkat Lunak: Y.S.; Validasi: K.B.R. dan L.K.C.; Analisis Formal: H.K. dan J.H.; Investigasi: K.B.R.; Sumber daya: L.K.C.; Kurasi Data: L.K.C.; Penulisan Draf Awal: Y.S. dan H.K.; Peninjauan dan Penyuntingan Tulisan: Y.S. dan H.K.; Visualisasi: L.K.C.; Semua penulis, K.B.R., L.K.C., Y.S., H.K., dan J.H., telah membaca dan menyetujui naskah yang telah diterbitkan.

5.2. Pernyataan Ketersediaan Data

Data yang disajikan dalam penelitian ini tersedia berdasarkan permintaan dari penulis yang bersangkutan.

5.3. Dana

Para penulis tidak menerima dukungan keuangan untuk penelitian, kepenulisan, dan/atau publikasi artikel ini.

5.4. Pernyataan Dewan Peninjau Institusi

Tidak berlaku.

5.5. Pernyataan Persetujuan Berdasarkan Informasi

Tidak berlaku.

5.6. Pernyataan Kepentingan Bersaing

Para penulis menyatakan bahwa mereka tidak memiliki kepentingan keuangan yang bersaing atau hubungan pribadi yang dapat mempengaruhi pekerjaan yang dilaporkan dalam makalah ini.

Semua publikasi yang dikutip dalam teks harus dimasukkan sebagai daftar referensi. Referensi diberi nomor urut saat muncul dalam teks. Nomor referensi ditunjukkan dalam tanda kurung. Harap pastikan bahwa setiap referensi yang dikutip dalam teks juga ada dalam daftar referensi (dan sebaliknya). Setiap referensi yang dikutip dalam abstrak harus diberikan secara lengkap. Hasil yang tidak dipublikasikan dan komunikasi pribadi tidak direkomendasikan dalam daftar referensi, tetapi dapat disebutkan dalam teks. Jika referensi ini dimasukkan dalam daftar referensi, mereka harus mengikuti referensi standar gaya jurnal dan harus memasukkan substitusi dari tanggal publikasi dengan ”hasil yang tidak dipublikasikan” atau ”komunikasi pribadi”.

DAFTAR PUSTAKA

[1] S. Parulian, D. A. Pratiwi, and M. C. Yustina, “Studi tentang ancaman dan solusi serangan siber di indonesia,” *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)*, vol. 1, no. 2, pp. 85–92, 2021.

[2] Z. Setiawan, A. Hiswara, and H. N. Muthmainah, “Mengoptimalkan jaringan sensor nirkabel dalam aplikasi monitor lingkungan dengan teknologi iot di indonesia,” *Jurnal Multidisiplin West Science*, vol. 2, no. 10, pp. 858–867, 2023.

[3] A. S. R. KK and H. N. Maharani, “Inovasi dan pengembangan produk keuangan syariah: Tantangan dan prospek di era revolusi industri 4.0,” *Jurnal Ilmiah Edunomika*, vol. 8, no. 1, 2023.

[4] M. Linda, “Inovasi dalam keamanan digital untuk pengguna aplikasi perbankan,” *Jurnal Inovasi Teknologi*, vol. 16, no. 4, pp. 132–150, 2023.

[5] M. Z. Ulhaq and M. R. Al Fajar, “Peluang dan tantangan bank syariah di era digital,” *J-ESA (Jurnal Ekonomi Syariah)*, vol. 5, no. 1, pp. 49–61, 2022.

[6] A. Zuhra and M. L. I. Nasution, “Penyelesaian masalah m-banking nasabah pt. bsi,” *Musytari: Neraca Manajemen, Akuntansi, dan Ekonomi*, vol. 3, no. 9, pp. 81–90, 2024.

[7] R. Hendra, “Tantangan dalam implementasi kebijakan keamanan data mobile banking,” *Jurnal Manajemen Keuangan Digital*, vol. 14, no. 2, pp. 85–100, 2022.

[8] N. Fitriani, “Solusi keamanan data dalam mobile banking melalui teknologi enkripsi,” *Jurnal Teknologi Informasi dan Keamanan Siber*, vol. 19, no. 4, pp. 142–160, 2023.

[9] M. A. Faizal, Z. Faizatul, B. N. Asiyah, and R. Subagyo, “Analisis risiko teknologi informasi pada bank syariah: Identifikasi ancaman dan tantangan terkini,” *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam*, vol. 5, no. 2, pp. 87–100, 2023.

[10] J. Smith and L. Davis, “Cybersecurity in mobile banking: Threats and solutions,” *Journal of Cybersecurity*, vol. 12, no. 3, pp. 120–135, 2020.

[11] J. Brown and E. White, “Mobile banking security: An overview of best practices,” *Journal of Financial Security*, vol. 8, no. 2, pp. 45–60, 2019.

[12] M. Lee and J. Kim, “Phishing attacks in mobile banking: Risks and countermeasures,” *Journal of Information Security*, vol. 29, no. 4, pp. 220–235, 2021.

[13] R. T. Tambunan and M. I. P. Nasution, “Tantangan dan strategi perbankan dalam menghadapi perkembangan transformasi digitalisasi di era 4.0,” *Sci-Tech Journal*, vol. 2, no. 2, pp. 148–156, 2023.

[14] X. Wang and D. Li, "Risk management in mobile banking: Challenges and opportunities," *Journal of Financial Technology*, vol. 14, no. 2, pp. 95–110, 2022.
[15] L. Garcia and A. Hernandez, "Biometric authentication in mobile banking: Security and usability," *International Journal of Financial Technology*, vol. 15, no. 1, pp. 75–88, 2020.
[16] M. Zulfan, "Analisis kebijakan keamanan dalam aplikasi perbankan digital di indonesia," *Jurnal Manajemen Teknologi*, vol. 15, no. 1, pp. 50–65, 2023.
[17] R. Andika, "Risiko keamanan pada pengguna mobile banking di indonesia: Tantangan dan solusi," *Jurnal Teknologi Informasi dan Keamanan*, vol. 19, no. 1, pp. 145–160, 2024.
[18] A. R. Maulidah, R. P. Astuti, K. Nisa, W. Erlangga, and E. Hambarwati, "Perkembangan sistem pembayaran digital: Pada era revolusi industri 4.0 di indonesia," *Jurnal Ekonomi Dan Bisnis Digital*, vol. 1, no. 4, pp. 798–803, 2024.
[19] R. Ihsan, "Peluang dan tantangan penggunaan blockchain technology pada perbankan syariah di indonesia," *Eqien-Jurnal Ekonomi dan Bisnis*, vol. 11, no. 03, pp. 1037–1049, 2022.
[20] M. A. Rahman and K. Astria, "Dampak fintech terhadap perkembangan perbankan," *Ekonomi Bisnis*, vol. 29, no. 1, pp. 12–19, 2023.
[21] A. Prima, "Implementasi teknologi biometrik dalam keamanan aplikasi perbankan digital," *Jurnal Teknologi Finansial dan Keamanan*, vol. 13, no. 4, pp. 125–140, 2023.
[22] A. Rizal, "Risiko keamanan siber dalam mobile banking dan solusi penanganannya," *Jurnal Keamanan Informasi*, vol. 8, no. 2, pp. 75–90, 2022.
[23] C. Jones and S.-M. Park, "Biometric authentication in mobile banking: Enhancing user trust," *Journal of Digital Security*, vol. 16, no. 4, pp. 200–215, 2019.
[24] I. Salim, "Peran edukasi pengguna dalam meningkatkan keamanan mobile banking," *Jurnal Pendidikan Teknologi*, vol. 10, no. 1, pp. 112–125, 2024.
[25] D. Ramdhan, "Kesiapan bank di indonesia dalam menghadapi ancaman keamanan siber pada mobile banking," *Jurnal Keamanan Siber Indonesia*, vol. 12, no. 2, pp. 55–70, 2023.
[26] W. Zhang and H. Liu, "Challenges and solutions in mobile banking: A review of security threats," *Journal of Cybersecurity Research*, vol. 25, no. 1, pp. 45–60, 2021.
[27] D. Williams and R. Johnson, "User awareness and its impact on mobile banking security," *Journal of Cyber Threat Intelligence*, vol. 13, no. 3, pp. 55–70, 2019.
[28] W. Chen and Y. Zhang, "The importance of end-to-end encryption in mobile banking security," *Journal of Cryptographic Security*, vol. 27, no. 1, pp. 65–80, 2021.
[29] L. Nguyen and M. Hoang, "The role of user education in enhancing mobile banking security," *Journal of Digital Banking*, vol. 18, no. 2, pp. 89–105, 2022.
[30] R. Kumar and S. Patel, "Regulation and security in mobile banking: A global perspective," *International Journal of Banking Regulation*, vol. 11, no. 3, pp. 145–160, 2020.
[31] S. Taylor and P. Brown, "Malware in mobile banking applications: Detection and prevention," *Cybersecurity Technology Journal*, vol. 22, no. 4, pp. 110–125, 2021.
[32] F. Ahmed and A. Tariq, "Security challenges in mobile banking: A case study of biometric authentication," *Journal of Financial Security and Data Protection*, vol. 9, no. 3, pp. 210–225, 2020.
[33] R. Clark and G. Evans, "Privacy and data protection in mobile banking: A regulatory review," *International Journal of Information Security*, vol. 28, no. 2, pp. 112–125, 2022.
[34] M. Ramirez and K. Carter, "The impact of cybersecurity education on mobile banking users," *Journal of Educational Technology and Security*, vol. 19, no. 3, pp. 155–170, 2021.