JoSES: Journal of Sharia Economics Scholar
Volume 2, Nomor 2, June 2023, Halaman 79-83

ISSN: 2302-6219
DOI: https://doi.org/10.5281/zenodo.12527995

Analisis Keamanan Data Pada Aplikasi Mobile Banking

Rohid Akbar[1], Muhammad Irwan Padli Nasution[2]
[12]Program Studi Manajemen, Fakultas Ekonomi Dan Bisnis Islam, Universitas Islam Negeri Sumatera Utara
[1]Email; rohidmehra1445@gmsil.com[1], irwannst@uinsu.ac.id[2]

Abstract

This article uses a qualitative methodology with literature review or literature research. Literature research is a research object or library-type information collected through the collection of scientific materials or writings. The purpose of this analysis is to find out how mobile banking applications can be protected from cyber attacks and data security Mobile banking applications must have a strong and effective security system to protect user information. Some methods to improve the security of mobile banking applications include blockchain technology, two-factor security, and periodic security testing. When analyzing data security, several factors that affect data security should be taken into account, such as authentication systems, encryption systems, and threat detection systems.
Keywords : *data security, mobile banking, finance*

Abstrak

Artikel ini menggunakan metodologi kualitatif dengan tinjauan literatur atau penelitian kepustakaan. Penelitian kepustakaan adalah suatu objek penelitian atau informasi yang bersifat kepustakaan yang dikumpulkan melalui pengumpulan bahan-bahan atau tulisan-tulisan ilmiah. Tujuan dari analisis ini adalah untuk mengetahui bagaimana aplikasi mobile banking dapat terlindungi dari serangan siber dan keamanan data Aplikasi mobile banking harus memiliki sistem keamanan yang kuat dan efektif untuk melindungi informasi pengguna. Beberapa metode untuk meningkatkan keamanan aplikasi mobile banking antara lain dengan teknologi blockchain, keamanan dua faktor, dan pengujian keamanan secara berkala. Ketika menganalisis keamanan data, beberapa faktor yang mempengaruhi keamanan data harus diperhitungkan, seperti sistem otentikasi, sistem enkripsi, dan sistem deteksi ancaman.
Kata kunci : *keamanan data, mobile banking, keuangan*

Article Info
Received date: 08 June 2024 Revised date: 18 June 2024 Accepted date: 22 June 2024

PENDAHULUAN

Saat ini masyarakat hidup pada dua periode yang tengah tumbuh dengan cepat, yaitu globalisasi dan era modern. Situasi di mana perkembangan teknologi dikendalikan oleh pemikiran manusia yang semakin maju. Perkembangan teknis pada awalnya agak lambat, tetapi semakin majunya peradaban dan budaya. mendukung perkembangan teknologi yang pesat.(Arum et al., 2022) Internet merupakan keperluan utama terutama bagi pengguna teknologi informasi. Sebagai salah satu bentuk perkembangan teknologi, Internet Telah menyebar ke segala ranah kehidupan, termasuk dalam bisnis, pendidikan, dan kesehatan. Ini juga memiliki dampak besar pada lembaga keuangan. salah satunya perbankan. Dunia perbankan tidak ingin tertinggal dalam hal teknologi dan informasi. Faktanya, industri perbankan saat ini telah meningkatkan layanan perbankan sesuai dengan kemajuan teknologi dan informasi. Contohnya, jika diluncurkan jasa yang disebut Electronic Banking (E-Banking)di dunia perbankan.(Hasdiana, 2018)

Mobile banking, atau lebih dikenal M-banking adalah sebuah layanan perbankan yang menggunakan perangkat seluler, seperti telepon genggam. Bank yang menawarkan layanan ini memungkinkan untuk melakukan transaksi perbankan dengan kemudahan, kenyamanan, dan keamanan.. Layanan perbankan melalui ponsel mempermudah klien untuk melakukan transaksi seperti pengecekan saldo dan transfer rekening, dll. Berdasarkan survei Populix 2022 10 aplikasi mobile banking yang paling populer di Indonesia adalah 50% dari orang yang menggunakan BCA Mobile, 25% menggunakan Brimo, 24% menggunakan Livin' Mandir, dan BNI Mobile menempati

urutan keempat. Bank with 22% users followed by BSI 10%, CIMB Niaga has Octo Mobile and Permata Mobile 10%, BTN Mobile Banking 9%, BJB Bank DIGI and D-Mobile. Bank Danamon 2%. Dan sejauh ini setiap bank telah meningkatkan layanan mobile banking-nya untuk memudahkan pelanggan melakukan pembayaran. Beberapa alasan nasabah menggunakan mobile banking untuk aktivitas keuangannya di era digital termasuk kepraktisan (78%), efisiensi waktu (90%), kemudahan penggunaan (66%), kemudahan dalam melakukan transaksi keuangan (86%), dan berbagai kemudahan lainnya. 63% dari responden mengatakan bahwa mereka lebih menyukai produk yang memiliki lebih banyak fungsi, sementara 57% menyukai produk yang terintegrasi dengan toko online. Sebanyak 35% responden menginginkan produk yang terintegrasi dengan e-wallet, sementara 52% mengutamakan kenyamanan produk tersebut. (Lubis & Lukman, 2023)

Perkembangan teknologi informasi dan komunikasi telah mempengaruhi munculnya bentuk-bentuk kejahatan baru melalui cybercrime. Dalam layanan mobile banking, data pribadi dapat dicuri jika ponsel nasabah dimanfaatkan orang lain karena dipinjam, dicuri, atau hilang. Ancaman juga dapat timbul di dunia digital atau yang lebih sering disebut dengan cybercrime.. Beberapa kasus kejahatan siber berkaitan dengan kejahatan yang dilakukan oleh pelaku kejahatan di media sosial dan internet dan sedikit banyak terbukti merugikan keamanan nasional. Selain keamanan dan kerahasiaan, tujuan utama sistem mobile banking yang dibuat dan digunakan oleh nasabah bank saat menggunakan mobile banking adalah kesederhanaan dan kenyamanan perbankan. Keamanan data merupakan aspek yang sangat penting dalam aplikasi mobile banking. Informasi yang dikumpulkan oleh aplikasi mobile banking, seperti data pribadi, nomor rekening, dan informasi keuangan, sangatlah sensitif dan dapat digunakan oleh pihak luar untuk melakukan kejahatan keuangan. Oleh karena itu, aplikasi mobile banking harus memiliki sistem keamanan yang kuat dan efektif untuk melindungi informasi pengguna. (Arum et al., 2022)

Saat menganalisis keamanan data aplikasi seluler tertentu, akan mempertimbangkan beberapa faktor yang memengaruhi keamanan data, seperti sistem autentikasi, sistem enkripsi, dan sistem deteksi ancaman. Kami juga membahas beberapa metode untuk meningkatkan keamanan aplikasi mobile banking, seperti teknologi blockchain, keamanan dua faktor, dan pengujian keamanan rutin. Dengan demikian, analisis ini bertujuan untuk memahami bagaimana aplikasi tersebut berfungsi. mobile banking dapat terlindungi dari serangan cyber dan keamanan data serta bagaimana cara melindungi informasi yang dikumpulkan oleh aplikasi dengan benar. Dengan cara ini, aplikasi mobile banking dapat menjadi lebih aman dan andal bagi pengguna serta meningkatkan kepercayaan pengguna terhadap aplikasi tersebut. (Rahmahdhani et al., 2023)

METODE

Artikel ini menggunakan metodologi kualitatif, Tujuan dari metode kualitatif adalah untuk memahami cara pandang suatu masyarakat atau individu terhadap suatu permasalahan tertentu. Peneliti perlu memiliki pemahaman yang memadai tentang topik penelitian dan kemampuan untuk mendapatkan informasi yang relevan, membatasi asumsi, serta menulis dengan persuasif agar pembaca dapat merasakan hal yang sama. . Dimana penulis mengumpulkan informasi “ analisis keamanan data pada aplikasi mobile banking. Semua artikel yang digunakan berasal dari majalah-majalah ternama, yang misalnya memiliki informasi mesin pencari berdasarkan abjad. Google Scholar, web dan Mendeley Electronics digunakan secara induktif untuk menghindari pertanyaan lebih lanjut.

HASIL DAN PEMBAHASAN

Definisi Keamanan data

Keamanan informasi dan data adalah tindakan yang diambil dengan bantuan peraturan dan teknologi untuk melindungi informasi dari kehilangan, perubahan, dan penyebaran yang disengaja atau tidak disengaja. Keamanan data melibatkan mengetahui data apa yang Anda miliki dan di mana lokasinya, serta mengidentifikasi risiko data. Tujuan dari keamanan data adalah untuk mencegah kemungkinan terjadinya kerusakan material, mengurangi resiko penyalahgunaan data dan mengurangi kemungkinan terjadinya kejahatan. Keamanan data sangat penting karena pencurian data meningkat secara signifikan. Keamanan data membantu mencegah penggunaan data yang tidak sah, mengidentifikasi dan mengurangi risiko data, dan memahami konteks aktivitas pengguna dan data.

(Mukhtisar et al., 2021)

Mobile Banking Development

Pada tahun 1995, Excelcom memperkenalkan layanan mobile banking (M-Banking) untuk pertama kalinya. Dengan beragam jawaban. Hampir semua bank sekarang ingin meraih kepercayaan dari setiap pelanggan mereka sebelum mulai m-banking. And one way to do this is by utilizing technology. Menurut data survei MARS Indonesia tahun 2012, di lima kota (Jakarta, Bandung, Semarang, Surabaya dan Medan), jumlah pelanggan yang menyadari layanan mobile perbankan meningkat drastis menjadi 40,4 persen. Atau naik sebesar 24,9% dari tahun 2008 yang hanya mencakup 35,5% dari 1.710 nasabah yang disurvei, separuhnya mengakui familiar dengan layanan mobile banking.

Model Keamanan data online mobile banking

Model yang saat ini diperkenalkan dalam sistem perbankan online dirancang dengan beberapa lapisan keamanan informasi, terdiri dari berbagai solusi dan mekanisme paralel. Tujuannya adalah untuk melindungi aplikasi perbankan dan data pelanggan serta menyediakan identifikasi, otentikasi, dan otorisasi. Keamanan informasi online perbankan melibatkan:

1. Sertifikat digital
   Sertifikat digital dipergunakan untuk memvalidasi atau mengakui keabsahan antara pengguna dan sistem perbankan yang bersangkutan. Keabsahan otentikasi ini tergantung pada PKI dan CA yang diberi kepercayaan untuk menyertifikasi sertifikat digital.
2. . Kartu kata sandi satu kali:
   Kartu kata sandi satu kali merupakan alternatif yang lebih terjangkau untuk menciptakan kata sandi dinamis dan juga menawarkan verifikasi kedua. Di beberapa sistem perbankan, kata sandi yang dihasilkan oleh kartu OTP (One Time Password) dapat digunakan beberapa kali sebelum dihancurkan, sehingga rentan terhadap serangan keamanan sementara.
3. Perlindungan browser
   Pengguna browser terlindungi dari malware dengan memonitor ruang memori yang digunakan oleh browser untuk mendeteksi dan mencegah malware serta menghindari pencurian informasi sensitif seperti nama pengguna. kata sandi.
4. Keyboard virtual:
   Keyboard virtual dikembangkan untuk mencegah penggunaan keyboard (perekaman data yang dimasukkan ke dalam perangkat lunak). Alat ini biasanya merupakan perangkat lunak berbasis Java yang mendukung berbagai browser web.
5. Pendaftaran perangkat:
   Metode ini menghalangi perangkat yang belum diidentifikasi atau didaftarkan dalam sistem dari mengakses sistem perbankan. Perangkat ini memanfaatkan pemindai sidik jari untuk mengenali pengguna.
6. CAPTCHA
   (Fully Automated Public Turing Test To Tell Computers and Humans Apart) adalah mekanisme yang memvalidasi bahwa individu yang mengakses sebuah situs web adalah manusia, bukan komputer. program komputer. Sistem ini bekerja dengan menampilkan gambar atau teks yang terdistorsi sehingga menyulitkan program komputer untuk membedakannya, namun manusia dapat membedakannya. Pengguna harus mengenali teks atau gambar yang ditampilkan untuk memastikan bahwa mereka adalah orang yang sah.
7. Layanan pesan singkat (SMS):
   Layanan pesan singkat (SMS) adalah metode yang digunakan di bank Internet yang memberi tahu nasabah bank tentang transaksi yang akan dilakukan melalui pesan teks. Pesan teks ini menyediakan saluran verifikasi lain untuk transaksi bank, di mana sistem perbankan online mengirimkan serangkaian karakter dalam pesan teks kepada pengguna (pelanggan bank), yang harus dikirimkan ke otoritas verifikasi melalui bank online selama proses transaksi.
8. Identifikasi perangkat:
   Identifikasi perangkat biasanya diterapkan bersamaan dengan registrasi perangkat, tetapi juga dapat digunakan sebagai solusi independen di dalam sistem perbankan online, dengan tujuan mempermudah akses bagi nasabah bank. Model ini mengidentifikasi asal dan keaslian nasabah bank berdasarkan karakteristik fisik perangkat yang digunakan.
9. riwayat data perangkat.

Dengan menggunakan beberapa model keamanan data seperti itu, aplikasi perbankan dan data pelanggan dapat lebih terlindungi dari serangan keamanan data dan kejahatan dunia maya.

Strategi Mencegah kejahatan mobile banking

Aplikasi mobile banking dapat dilindungi dari serangan cyber dan keamanan data dengan melakukan langkah-langkah berikut:

1. Otentikasi dua faktor (2FA): Aplikasi perbankan seluler biasanya menggunakan 2FA, seperti verifikasi SMS yang menyertakan kata sandi satu kali (OTP), untuk memastikan bahwa setiap transaksi dilakukan oleh pengguna yang berwenang
2. Enkripsi data:data pengguna dienkripsi dan dikirimkan melalui saluran perbankan yang sangat aman untuk melindungi dari serangan malware.
3. pembaruan rutin: Pastikan untuk memperbarui aplikasi mobile banking Anda. Setiap versi terbaru hadir dengan fitur tambahan dan sistem keamanan tingkat lanjut.
4. Koneksi Internet Aman: Jangan menggunakan jaringan Internet atau Wi-Fi di tempat umum untuk transaksi online. Gunakan internet yang aman dan terenkripsi sebagai gantinya.
5. Kata sandi yang kuat: Untuk mencegah peretasan, gunakan kata sandi yang kuat dan ubah kata sandi Anda secara berkala.
6. Hindari Wi-Fi Publik: Hindari penggunaan Wi-Fi publik untuk mengakses aplikasi mobile banking. Jika Anda harus menggunakan wifi publik, pastikan untuk menggunakan VPN yang aman.
7. Pantau transaksi Anda:Pastikan Anda memeriksa transaksi Anda secara rutin untuk mengidentifikasi transaksi yang mencurigakan. segera hubungi contact center bank.
8. Penyimpanan aman: Simpan ponsel Anda di tempat yang aman untuk mencegah kehilangan atau pencurian data.
9. Anti-phishing: Jangan tertipu oleh email atau pesan yang mengaku sebagai bank Anda dan meminta Anda memberikan informasi pribadi. Pastikan Anda hanya menggunakan aplikasi mobile banking dengan link resmi bank Anda.
10. Dukungan pelanggan: Jika Anda mengalami masalah dengan aplikasi seluler, pastikan untuk menghubungi layanan pelanggan bank Anda.

Dengan mengikuti panduan ini, Anda dapat memastikan keamanan transaksi pembayaran Anda dan menghindari serangan cyber terhadap aplikasi mobile banking. (Rahayu, 2021)

SIMPULAN

Dapat disimpulkan bahwa analisis keamanan aplikasi mobile banking sangat penting untuk melindungi informasi sensitif seperti data pribadi, nomor rekening dan informasi keuangan. Aplikasi mobile banking harus memiliki sistem keamanan yang kuat dan efektif untuk melindungi informasi pengguna. Beberapa metode untuk meningkatkan keamanan aplikasi mobile banking meliputi teknologi blockchain, keamanan dua faktor, dan pengujian keamanan berkala. Saat menganalisis keamanan data, beberapa faktor yang mempengaruhi keamanan data harus diperhitungkan, seperti sistem otentikasi, sistem enkripsi, dan sistem deteksi ancaman. Selain itu, beberapa model keamanan online mobile banking seperti sertifikat digital, kartu kata sandi satu kali, perlindungan browser, keyboard virtual, registrasi perangkat, CAPTCHA, layanan SMS dan identifikasi perangkat dapat digunakan untuk melindungi aplikasi perbankan dan data pelanggan. Strategi pencegahan kejahatan mobile banking mencakup otentikasi dua faktor, verifikasi pesan teks dan penggunaan teknologi blockchain. Dengan cara ini, aplikasi mobile banking dapat menjadi lebih aman dan andal bagi pengguna serta meningkatkan kepercayaan pengguna terhadap aplikasi tersebut.

REFERENSI

Arum, S., Kaltsum, D., & Muslichah, I. (2022). *Artikel Hasil Penelitian Mobile Banking*. *01*(02), 31–46. https://journal.uii.ac.id/selma/index

Hasdiana, U. (2018). No keamanan layanan internet banking dalam transaksi perbankanTitle. *Analytical Biochemistry*, *11*(1), 1–5. http://link.springer.com/10.1007/978-3-319-59379-1%0Ahttp://dx.doi.org/10.1016/B978-0-12-420070-8.00002-

Lubis, D. yanti, & Lukman, S. (2023). Pengaruh Persepsi Kegunaan, Kemudahan dan Keamanan Terhadap Kepuasan Nasabah Menggunakan Mobile Banking. *Jeksya Jurnal Ekonomi Dan Keuangan Syariah*, *vol.2*(2), 443–456.

Mukhtisar, M., Tarigan, I. R. R., & Evriyenni, E. (2021). Pengaruh Efisiensi, Keamanan Dan Kemudahan Terhadap Minat Nasabah Bertransaksi Menggunakan Mobile Banking (Studi Pada Nasabah Bank Syariah Mandiri Ulee Kareng Banda Aceh). *Jihbiz: Global Journal of Islamic Banking and Finance.*, *3*(1), 56. https://doi.org/10.22373/jihbiz.v3i1.9632

Rahayu, H. H. S. W. (2021). Analisis Perlindungan Kerahasiaan Data Pribadi Pada Nasabah Pengguna Produk Layanan Mobile Banking Bank Milik Pemerintah Daerah Aceh. *Jurnal Ilmiah Mahasiswa Bidang Hukum Keperdataan*, *5*(Vol 5, No 2: Mei 2021), 328–337. http://jim.unsyiah.ac.id/perdata/article/view/19196/8850

Rahmahdhani, D. N., Nasution, M. I. P., & Sundari, S. S. A. (2023). Perlindungan Data Privasi Yang Dilakukan Perbankan Terhadap Penggunaan Layanan Mobile Banking. *JUEB : Jurnal Ekonomi Dan Bisnis*, *2*(2), 88–96. https://doi.org/10.57218/jueb.v2i2.693