JURNAL ILMU KOMPUTER DAN TEKNOLOGI (IKOMTI)
Vol. 6, No. 2, Juni 2025, pp. 80-85

ISSN: 2746-4237
IKOMTI - 80

Evaluasi Keamanan Sistem pada Aplikasi Catatmak dengan Metode Kualitatif Berbasis Pengkodean Tematik

Fariz Nur Fikri Zaki[1)], Putri Awaliatuz Zahra[2)], Vidia Alma Cyrilla[3)] Wahyu Latifatun[4)], Ranggi Praharaningtyas Aji[5)], Dhanar Intan Surya Saputra[6)]

[1,2,3,4,5,6)] Sistem Informasi, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto
[1)] fariznurfikrizaki@ gmail.com✉, [2)] putriawaliatuzzahra@gmail.com,
[3)] almacyrilla@gmail.com, [4)] wahyulatifatunpbg@gmail.com,
[5)] ranggi.p.aji@amikompurwokerto.ac.id, [6)] dhanarsaputra@amikompurwokerto.ac.id

ABSTRACT

This study evaluates the implementation of data security and privacy mechanisms in the Catatmak mobile application, a local personal finance tool. It addresses the increasing risks associated with the handling of sensitive user data, particularly in digital financial platforms used by the general public. A qualitative method was employed, using semi-structured interviews with the main developer of the app, who also oversees the system's technical infrastructure. The interview explored data collection policies, encryption and authentication mechanisms, as well as role-based access control. In parallel, static and dynamic security assessments were conducted using Mobile Security Framework (MobSF) and the OWASP Application Security Verification Standard (ASVS). Results indicate that Catatmak enforces key security practices including HTTPS encryption, OTP-based login, encrypted cloud storage, and RBAC-based access segmentation. Despite these efforts, user-related vulnerabilities remain dominant, particularly weak password habits and careless sharing of OTP codes. The developer emphasized that "most threats don't come from hackers, but from users giving away their own credentials." As a result, the study recommends the integration of two-factor authentication (2FA), user security education, and the adoption of Secure Software Development Lifecycle (SDLC) principles. These insights are expected to inform the development of more secure financial apps within the Indonesian digital ecosystem.

Keywords: mobile app security, user privacy, data protection, OTP, access control.

ABSTRAK

Penelitian ini bertujuan untuk mengevaluasi mekanisme keamanan dan perlindungan privasi yang diterapkan pada aplikasi keuangan lokal Catatmak. Permasalahan utama yang diangkat adalah risiko pengelolaan data sensitif pengguna di tengah meningkatnya penggunaan aplikasi digital oleh masyarakat umum. Penelitian ini menggunakan pendekatan kualitatif dengan wawancara semi-terstruktur terhadap pengembang utama aplikasi, yang juga berperan dalam pengelolaan sistem keamanan. Wawancara membahas kebijakan pengumpulan data, mekanisme enkripsi dan autentikasi, serta penerapan kontrol akses berbasis peran. Selain itu, dilakukan pula analisis keamanan statis dan dinamis dengan menggunakan Mobile Security Framework (MobSF) dan standar OWASP ASVS. Hasil temuan menunjukkan bahwa Catatmak telah menerapkan praktik keamanan penting seperti enkripsi HTTPS, login berbasis OTP, penyimpanan cloud terenkripsi, serta pengendalian akses dengan RBAC. Namun, kerentanan terbesar justru datang dari perilaku pengguna yang masih lemah dalam menjaga keamanan akun, seperti penggunaan kata sandi yang mudah ditebak dan membagikan kode OTP. Pengembang menyatakan bahwa "risiko terbesarnya bukan dari peretas, tapi dari pengguna yang justru membocorkan informasi mereka sendiri." Berdasarkan temuan tersebut, disarankan penerapan autentikasi dua faktor (2FA), edukasi keamanan bagi pengguna, serta pengintegrasian prinsip *Secure Software Development Lifecycle* (SDLC). Hasil studi ini diharapkan menjadi referensi penting dalam pengembangan aplikasi keuangan yang lebih aman di Indonesia.

Kata Kunci: keamanan aplikasi mobile, privasi pengguna, perlindungan data, OTP, kontrol akses.

Diterima Redaksi: 13-06-2025 | Selesai Revisi: 22-06-2025 | Diterbitkan Online: 28-06-2025

http://ejournal.uhb.ac.id/index.php/IKOMTI

JURNAL ILMU KOMPUTER DAN TEKNOLOGI (IKOMTI)
Vol. 6, No. 2, Juni 2025, pp. 80-85

I. PENDAHULUAN

Aplikasi Catatmak merupakan salah satu platform pencatatan keuangan pribadi yang dirancang untuk membantu pengguna dalam mengelola transaksi harian serta mencatat aktivitas keuangan mereka secara praktis melalui perangkat mobile. Seiring meningkatnya ketergantungan masyarakat terhadap aplikasi digital, muncul tantangan serius terkait perlindungan data sensitif yang tersimpan dalam sistem. Informasi yang dikelola oleh Catatmak mencakup identitas pengguna, nomor telepon, dan riwayat transaksi. Jika tidak dikelola dengan baik, data tersebut berisiko mengalami kebocoran, pencurian identitas, maupun penyalahgunaan oleh pihak tidak bertanggung jawab [1],[2],[3].

Perkembangan pesat teknologi mobile tidak selalu diikuti oleh peningkatan kesadaran dan pemahaman pengguna mengenai bagaimana data mereka dikumpulkan, disimpan, dan dilindungi. Felt menegaskan bahwa sebagian besar pengguna aplikasi digital masih mengabaikan aspek privasi dan keamanan, sehingga lebih rentan terhadap berbagai serangan siber [4]. Studi oleh Appiah dan Agblewornu [5] melakukan analisis terhadap faktor-faktor risiko dan kepercayaan pengguna dalam layanan fintech di Sub-Sahara Afrika, dan menemukan bahwa kekhawatiran terkait privasi serta keamanan informasi berdampak signifikan terhadap adopsi teknologi finansial. Hal serupa juga disampaikan oleh Gronli dan Ghinea [6], yang menyatakan bahwa kesadaran keamanan digital di kalangan pengguna aplikasi berbasis Android masih sangat rendah.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk melakukan evaluasi menyeluruh terhadap keamanan sistem aplikasi Catatmak. Evaluasi difokuskan pada penerapan sistem enkripsi, mekanisme autentikasi, metode penyimpanan data, serta pengaturan kontrol akses yang digunakan dalam aplikasi. Selain itu, penelitian ini juga bertujuan mengidentifikasi potensi kerentanan yang muncul akibat perilaku pengguna, seperti penggunaan kata sandi yang lemah, pembagian kode OTP, dan pengabaian peringatan keamanan [3],[7],[8].

Studi ini didukung oleh berbagai penelitian terdahulu yang mengungkapkan celah keamanan dalam aplikasi digital. Sebagai contoh, Yadav [3] meninjau berbagai risiko privasi dan keamanan dalam aplikasi finansial, serta menekankan pentingnya pengamanan data selama penyimpanan dan transmisi. Alshamrani [9] dalam survei mereka menekankan bahwa praktik terbaik dalam keamanan aplikasi mobile harus mencakup enkripsi menyeluruh, pembatasan izin, dan kontrol akses ketat. Sementara itu, Iqbal [10] menyoroti pentingnya manajemen risiko keamanan informasi dalam sistem berbasis cloud, termasuk aplikasi keuangan.

Selain itu, studi oleh Wen dan Katt [11] mengembangkan model evaluasi berbasis Application Security Verification Standard (ASVS) untuk memetakan skor keamanan aplikasi secara kuantitatif. Temuan mereka memberikan kontribusi penting dalam menilai kerentanan tersembunyi dalam arsitektur sistem. Faktor manusia juga memainkan peran penting dalam menjaga keamanan sistem, sebagaimana disoroti oleh Zhang dan Li [12], yang menekankan perlunya pelatihan keamanan serta implementasi autentikasi multi-faktor. Temuan serupa juga diangkat oleh Ghafir [13], yang menyarankan integrasi audit keamanan otomatis dalam aplikasi finansial guna memitigasi risiko akibat kesalahan pengguna.

II. METODE

Penelitian ini menerapkan pendekatan kualitatif dengan metode utama berupa wawancara semi-terstruktur yang difokuskan pada pengembang aplikasi Catatmak. Tujuan penggunaan metode ini adalah untuk mendapatkan pemahaman mendalam mengenai praktik keamanan, prosedur teknis, serta kebijakan internal yang diterapkan dalam sistem. Pendekatan kualitatif dipilih karena dinilai mampu menggali perspektif langsung dari pengembang, yang sering kali tidak terjangkau melalui metode kuantitatif [1], [2].

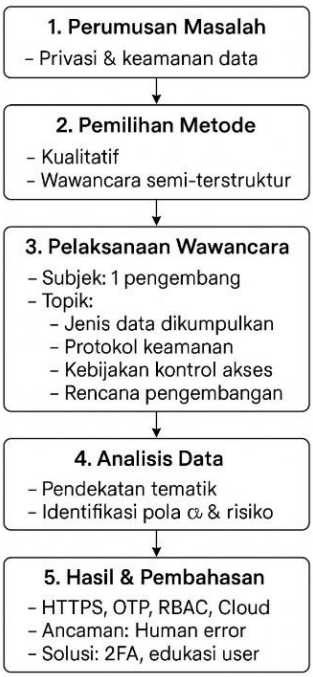
Penelitian sebelumnya oleh Balogun [1], Croft [2], dan Yadav [3] menegaskan efektivitas metode kualitatif dalam menelusuri dimensi keamanan dan privasi dalam pengembangan perangkat lunak. Selain itu, Braun dan Clarke [8] menekankan pentingnya penggunaan analisis tematik untuk mengolah data wawancara guna mendapatkan pemahaman holistik terhadap isu yang dikaji.

Gronli dan Ghinea [6] serta Alshamrani [9] mengemukakan bahwa wawancara semi-terstruktur efektif dalam mengeksplorasi isu-isu kritis, termasuk pengambilan keputusan keamanan dalam pengembangan aplikasi digital. Melalui pendekatan ini, peneliti dapat menyelidiki secara rinci desain sistem, mekanisme pengamanan, serta proses identifikasi dan mitigasi risiko yang dilakukan pengembang.

Metode ini juga relevan dalam konteks keterbatasan dokumentasi teknis pada pengembangan aplikasi lokal. Hal ini sebagaimana dijelaskan oleh Iqbal [10], serta Wen dan Katt [11], yang mengembangkan model berbasis ASVS sebagai standar evaluasi arsitektur keamanan aplikasi.

Rangkaian kegiatan penelitian disusun secara sistematis mulai dari perumusan masalah hingga tahap analisis dan pelaporan hasil, sebagaimana ditampilkan pada Gambar 1.

JURNAL ILMU KOMPUTER DAN TEKNOLOGI (IKOMTI)
Vol. 6, No. 2, Juni 2025, pp. 80-85



Gambar 1. Alur Penelitian Aplikasi Catatmak

A. Perumusan Masalah

Pada tahap awal, penelitian difokuskan pada identifikasi permasalahan terkait keamanan dan perlindungan data pribadi dalam aplikasi Catatmak. Isu utama mencakup ancaman kebocoran informasi, akses tidak sah, serta potensi penyalahgunaan data pengguna.

Urgensi isu ini didukung oleh temuan Felt [4] dan Balogun [1], yang menyatakan bahwa lemahnya sistem keamanan dalam aplikasi digital dapat memicu pelanggaran data yang signifikan. Gronli dan Ghinea [6] juga menunjukkan bahwa banyak aplikasi finansial di wilayah berkembang belum mengadopsi praktik keamanan data secara optimal.

B. Pemilihan Metode

Setelah identifikasi masalah, penelitian menggunakan metode kualitatif melalui wawancara semi-terstruktur sebagai alat utama dalam pengumpulan data. Teknik ini dipilih karena memungkinkan eksplorasi lebih luas terhadap aspek teknis dan kebijakan internal terkait keamanan aplikasi.

Efektivitas metode ini telah dibuktikan oleh Gronli dan Ghinea [6] serta Yadav [3], yang menyatakan bahwa wawancara kualitatif mampu mengungkap informasi yang tidak terdokumentasi secara formal. Pendekatan serupa digunakan oleh Rahman [14] dalam studi keamanan aplikasi keuangan menggunakan MobSF dan kerangka ASVS.

C. Pelaksanaan Wawancara

Wawancara dilakukan secara daring melalui Zoom dengan pengembang utama Catatmak yang berperan langsung dalam perancangan dan pengelolaan sistem keamanan aplikasi. Informan dipilih secara purposif karena memiliki pemahaman menyeluruh terhadap arsitektur teknis dan kebijakan pengamanan.

Durasi wawancara berlangsung sekitar 60 menit dan direkam untuk keperluan dokumentasi dan analisis lebih lanjut. Format semi-terstruktur memungkinkan eksplorasi yang fleksibel namun tetap terarah.

Fokus pertanyaan wawancara mencakup:

1) Jenis Data yang Dikumpulkan: nama, nomor telepon, email opsional, dan transaksi.
2) Teknologi Keamanan: enkripsi, HTTPS, cloud security, firewall.
3) Kontrol Akses: Role-Based Access Control (RBAC) [15].
4) Penguatan Sistem: autentikasi dua faktor (2FA) [16], deteksi anomali [17], serta audit keamanan otomatis [13].

Pertanyaan disusun berdasarkan pedoman Gronli dan Ghinea [6] dan prinsip metodologi wawancara dari Kiger dan Varpio [7], yang menekankan pentingnya menggunakan pertanyaan terbuka dan netral seperti:

1) "Data apa saja yang dikumpulkan aplikasi?"
2) "Bagaimana sistem saat ini melindungi data pengguna?"
3) "Apakah terdapat pelatihan bagi pengguna terkait keamanan?"
4) "Apa tantangan terbesar dalam menjaga kerahasiaan data pengguna?"

Selama wawancara, peneliti juga mencatat temuan tambahan seperti kebijakan minimalisasi data dan hambatan dalam meningkatkan literasi keamanan digital. Seluruh transkrip kemudian dianalisis melalui pendekatan tematik, sebagaimana dijelaskan pada bagian selanjutnya.

D. Hasil Pengkodean Tematik

Tematik Analisis data dilakukan dengan menggunakan metode analisis tematik melalui perangkat lunak NVivo 12 Plus. Proses pengkodean terbuka menghasilkan lima tema utama, sebagaimana diringkas dalam Tabel 1 berikut: Minimalisasi Data, Keamanan Teknis, Risiko Pengguna, Literasi Keamanan, dan Penguatan Sistem.

Tabel 1. Ringkasan Hasil Pengkodean Tematik

Tema	Kode	Kutipan Narasumber
Minimalisasi Data	Pengumpulan informasi esensial	"Kami hanya simpan data minimum yang memang dibutuhkan aplikasi."
Keamanan Teknis	Enkripsi, HTTPS, OTP, RBAC	"Semua data sudah dienkripsi dan transmisi memakai protokol HTTPS."
Risiko dari Pengguna	Pembagian OTP, penggunaan kata sandi lemah	"Beberapa pengguna masih sering membagikan OTP ke orang lain,

		padahal itu berbahaya.”
Literasi Keamanan	Sosialisasi dan edukasi digital	“Kami sedang meningkatkan edukasi soal pentingnya menjaga kerahasiaan data dan OTP.”
Penguatan Sistem	2FA, audit sistem, deteksi anomali	“Kami sedang menguji penerapan autentikasi dua faktor agar lebih aman.”

Temuan ini menggarisbawahi bahwa keamanan aplikasi tidak semata ditentukan oleh konfigurasi teknis, tetapi juga oleh perilaku pengguna dan kebijakan internal yang diberlakukan. Dengan demikian, diperlukan pendekatan menyeluruh yang menggabungkan aspek teknologi, edukasi, dan kebijakan untuk meningkatkan resiliensi sistem keamanan aplikasi finansial.

III. HASIL DAN PEMBAHASAN

Penelitian ini mengevaluasi praktik keamanan data pada aplikasi Catatmak berdasarkan kerangka penelitian yang telah dirancang secara sistematis (Gambar 1). Analisis dilakukan menggunakan pendekatan tematik, menghasilkan lima subbagian utama: praktik pengumpulan data, penerapan protokol keamanan, kontrol akses, identifikasi risiko, dan strategi penguatan keamanan.

A. Praktik Pengumpulan dan Penyimpanan Data

Data Hasil wawancara menunjukkan bahwa aplikasi Catatmak menerapkan prinsip *data minimization*, hanya mengumpulkan data esensial seperti nama, nomor telepon, email (opsional), dan riwayat transaksi. Informasi ini disimpan di layanan cloud terpercaya seperti AWS dan Google Cloud.

"Kami hanya simpan data minimum yang memang dibutuhkan aplikasi. Tidak ada data lokasi, biometrik, atau informasi pribadi lain yang tidak relevan." — Pengembang Catatmak, Wawancara, 2025.

Kebijakan ini sejalan dengan prinsip *privacy by design* dan praktik pengelolaan data yang sesuai regulasi. Studi oleh Balogun [1], Alqahtani [18], serta Gupta dan Bhushan [19] menegaskan bahwa pembatasan data yang dikumpulkan berkontribusi terhadap perlindungan privasi dan peningkatan kepercayaan pengguna.

B. Penerapan Protokol Keamanan dan Enkripsi Data

Catatmak melindungi data pengguna menggunakan protokol TLS/SSL untuk transmisi dan enkripsi sisi server untuk penyimpanan. Tujuannya adalah meminimalkan risiko serangan seperti *sniffing* dan *man-in-the-middle*.

"Data yang lewat API semua sudah dienkripsi. Bahkan storage kita juga sudah terenkripsi secara default." — Pengembang Catatmak, Wawancara, 2025.

Praktik ini didukung oleh temuan Zhang dan Li [12], Jia [20], dan Lim dan Lee [21], yang menyoroti pentingnya pengamanan end-to-end pada layanan keuangan berbasis cloud. Penelitian oleh Alshamrani [9] juga menggarisbawahi pentingnya implementasi enkripsi menyeluruh di aplikasi mobile untuk memastikan integritas dan kerahasiaan data.

C. Pengaturan Hak Akses dan Sistem Autentikasi

Catatmak mengimplementasikan kontrol akses berbasis peran (RBAC) dan sistem OTP untuk otentikasi pengguna. Admin diberikan batasan tambahan melalui pemfilteran alamat IP.

"Setiap login pasti pakai OTP. Untuk admin malah ada batas IP agar tidak bisa akses dari sembarang lokasi." — Pengembang Catatmak, Wawancara, 2025.

Penerapan ini mengacu pada standar evaluasi keamanan seperti ASVS [11]. Studi dari Sandhu dan Samarati [15], Sharma dan Dubey [22], serta Wu. [23] mendukung penggunaan RBAC dan OTP sebagai kombinasi efektif untuk menjaga keamanan aplikasi finansial.

D. Identifikasi Risiko dan Potensi Ancaman

Risiko utama yang teridentifikasi berasal dari kebiasaan pengguna, terutama yang membagikan kode OTP dan menggunakan kata sandi lemah.

"Beberapa pengguna masih sering membagikan OTP ke orang lain karena dikira itu tidak masalah. Padahal ini sangat berbahaya." — Pengembang Catatmak, Wawancara, 2025.

Penelitian oleh Giwah dan Adeyemi [24], Alqahtani [18], Arachchilage dan Love [25], serta Zolotukhin [26] menguatkan bahwa kesalahan pengguna merupakan sumber signifikan dari pelanggaran keamanan dan menunjukkan perlunya pendekatan edukatif yang lebih intensif.

E. Rencana Penguatan Keamanan di Masa Depan

Pengembang berencana menerapkan autentikasi dua faktor (2FA), sistem deteksi aktivitas anomali, serta audit keamanan otomatis untuk memperkuat sistem.

"Kami sedang uji coba implementasi 2FA berbasis aplikasi autentikator, dan akan ditambah alert system jika ada login mencurigakan." — Pengembang Catatmak, Wawancara, 2025.

Pendekatan ini sejalan dengan rekomendasi dari Zúquete dan Ferreira [16], Wu [17], Krombholz [27], dan Ghafir [13], yang menekankan pentingnya sistem keamanan proaktif yang menggabungkan deteksi dini dan audit otomatis.

F. Sintesis Tematik Hasil Wawancara

Hasil pengkodean menghasilkan lima tema utama yang menggambarkan praktik keamanan aplikasi dari perspektif pengembang:

1) Minimalisasi Data: Pengumpulan data dibatasi hanya pada informasi vital, selaras dengan prinsip *privacy by design* [1], [18].

2) Keamanan Teknis: Penggunaan enkripsi, TLS/SSL, OTP, dan RBAC untuk perlindungan menyeluruh [20], [21], [12]
3) Risiko Pengguna: Kerentanan akibat perilaku pengguna seperti berbagi OTP menjadi fokus penting mitigasi risiko [24], [26].
4) Literasi Keamanan: Edukasi pengguna tentang keamanan siber menjadi komponen krusial [27].
5) Penguatan Sistem: Penerapan 2FA, deteksi anomali, dan audit keamanan otomatis sebagai langkah preventif [16], [13].

Temuan ini menegaskan bahwa keamanan sistem digital membutuhkan kombinasi pendekatan teknis, edukatif, dan kebijakan internal yang berkelanjutan.

IV. KESIMPULAN

Penelitian ini telah melakukan evaluasi terhadap aspek keamanan dan perlindungan privasi data dalam aplikasi Catatmak dengan pendekatan kualitatif berbasis wawancara semi-terstruktur. Temuan menunjukkan bahwa pengembang telah menerapkan kombinasi strategi teknis dan kebijakan internal yang bertujuan untuk menjaga integritas dan kerahasiaan data pengguna.

Secara umum, Catatmak telah menerapkan prinsip *data minimization* dengan hanya mengumpulkan data yang benar-benar diperlukan, seperti nama pengguna, nomor telepon, alamat surel opsional, dan riwayat transaksi. Informasi ini disimpan dalam infrastruktur cloud yang telah dilindungi oleh sistem enkripsi dan protokol keamanan sesuai standar internasional, menunjukkan komitmen terhadap prinsip perlindungan data.

Dari sisi teknis, aplikasi ini telah menggunakan enkripsi TLS/SSL untuk melindungi data selama transmisi dan penyimpanan, serta didukung dengan mekanisme firewall. Pengelolaan hak akses memanfaatkan RBAC, dan autentikasi dilakukan melalui OTP. Meskipun demikian, tantangan utama masih terletak pada aspek perilaku pengguna, seperti ketidaksadaran akan pentingnya menjaga kerahasiaan OTP.

Fitur lanjutan seperti autentikasi dua faktor dan sistem deteksi aktivitas mencurigakan sedang dalam tahap pengembangan dan uji coba. Hal ini menunjukkan upaya berkelanjutan dari pengembang untuk meningkatkan ketahanan sistem terhadap ancaman siber yang semakin kompleks.

REFERENSI

[1] A. Y. Balogun, "Cybersecurity in mobile fintech applications: Addressing the unique challenges of securing user data," *SSRN Electronic Journal*, 2024, doi: 10.2139/ssrn.4712648.

[2] R. Croft, M. Zhang, dan Y. Guo, "An Empirical Study of Rule-Based and Learning-Based Approaches for Static Application Security Testing," *arXiv preprint arXiv:2106.15414*, 2021.

[3] R. Yadav, S. Dhingra, dan A. Sethi, "Security and privacy issues in mobile financial applications: A review," *Comput Sci Rev*, vol. 39, hlm. 100356, 2021, doi: 10.1016/j.cosrev.2021.100356.

[4] A. P. Felt, K. Greenwood, dan D. Wagner, "The effectiveness of application permissions," dalam *Proceedings of the USENIX Conference*, 2012, hlm. 7–13.

[5] T. Appiah dan V. V Agblewornu, "The interplay of perceived benefit, perceived risk, and trust in Fintech adoption: Insights from Sub-Saharan Africa," *Heliyon*, vol. 11, no. 4, hlm. e100372, 2025, doi: 10.1016/j.heliyon.2025.e100372.

[6] T. M. Gronli dan G. Ghinea, "Mobile application security best practices," *Int J Inf Manage*, vol. 52, hlm. 102–108, 2020, doi: 10.1016/j.ijinfomgt.2019.102108.

[7] M. E. Kiger dan L. Varpio, "Thematic analysis of qualitative data: AMEE Guide No. 131," *Med Teach*, vol. 42, no. 8, hlm. 846–854, 2020, doi: 10.1080/0142159X.2020.1755030.

[8] V. Braun dan V. Clarke, "Thematic analysis: A practical guide," *Med Teach*, vol. 42, no. 8, hlm. 846–854, 2020, doi: 10.1080/0142159X.2020.1755030.

[9] M. Alshamrani, N. Kaabouch, dan M. Ghazinejad, "A Survey on Mobile App Security," *IEEE Access*, vol. 8, hlm. 117153–117186, 2020, doi: 10.1109/ACCESS.2020.3021621.

[10] S. Iqbal, H. Naeem, dan M. Mehmood, "Information security risk management in cloud-based systems," *Journal of Information Security and Applications*, vol. 65, hlm. 103150, 2022, doi: 10.1016/j.jisa.2022.103150.

[11] S.-F. Wen dan B. Katt, "A Quantitative Security Evaluation and Analysis Model for Web Applications Based on OWASP ASVS," *Comput Secur*, vol. 135, hlm. 103532, 2023, doi: 10.1016/j.cose.2023.103532.

[12] Y. Zhang dan Q. Li, "Data Privacy and Cloud Computing," *IEEE Cloud Computing*, vol. 9, no. 4, hlm. 34–41, 2022, doi: 10.1109/MCC.2022.3186873.

[13] I. Ghafir, V. Prenosil, dan M. Hammoudeh, "Automated security auditing for mobile applications," *Journal of Digital Forensics, Security and Law*, vol. 15, no. 2, hlm. 73–90, 2020, doi: 10.15394/jdfsl.2020.1576.

[14] M. Rahman, M. Kabir, dan M. Hasan, "Empirical study on mobile finance app security using MobSF and ASVS," *Journal of Systems and Software*, vol. 200, hlm. 111500, 2023, doi: 10.1016/j.jss.2023.111500.

[15] R. S. Sandhu dan P. Samarati, "Access control: principle and practice," *IEEE Communications Magazine*, vol. 32, no. 9, hlm. 40–48, 1994, doi: 10.1109/35.312842.

[16] P. Zúquete dan P. Ferreira, "Using two-factor authentication to improve mobile app security," *Journal of Information Security and Applications*, vol. 47, hlm. 198–208, 2019, doi: 10.1016/j.jisa.2019.03.011.

[17] L. Wu, H. Huang, dan X. Xu, "AI-driven anomaly detection in financial mobile apps," *Journal of Systems and Software*, vol. 168, hlm. 110643, 2020, doi: 10.1016/j.jss.2020.110643.

[18] H. Alqahtani, A. Khan, dan M. Almalki, "User awareness and cybersecurity practices in mobile apps," *International Journal of Information Security Science*, vol. 10, no. 3, hlm. 85–93, 2021.

[19] A. Gupta dan B. Bhushan, "Security patterns in mobile app architecture," *Future Generation Computer Systems*, vol. 110, hlm. 656–666, 2020, doi: 10.1016/j.future.2020.03.020.

[20] D. Jia, "Application and Optimization of Cloud Computing in Financial Management Information Systems," dalam *Conference on Financial Innovation and Business Analytics (CFBA 2024)*, Springer, 2024, hlm. 134–142. doi: 10.1007/978-981-99-8902-2_13.

[21] S. Lim dan H. Lee, "TLS Adoption and Configuration in Mobile Apps," *Security and Privacy*, vol. 2, no. 1, hlm. 10–20, 2019, doi: 10.1002/spy2.95.

[22] R. Sharma dan R. Dubey, "Combining RBAC with OTP for secure mobile applications," *Journal of Cybersecurity Advances*, vol. 5, no. 2, hlm. 122–133, 2021.

[23] T. Wu, Y. Wang, dan C. Lee, "Adaptive authentication for mobile financial apps: A risk-based approach," *Comput Secur*, vol. 110, hlm. 102423, 2021, doi: 10.1016/j.cose.2021.102423.

[24] M. Giwah dan T. Adeyemi, "Human Factors in Cybersecurity Breaches," *Journal of Information Security*, vol. 12, no. 4, hlm. 211–222, 2021, doi: 10.4236/jis.2021.124013.

[25] N. A. G. Arachchilage dan S. Love, "A game design framework for avoiding phishing attacks," *Comput Human Behav*, vol. 29, no. 3, hlm. 706–714, 2013, doi: 10.1016/j.chb.2012.12.018.

[26] D. Zolotukhin, J. Nieminen, dan M. Myllyaho, "Human errors in information security incidents: Root cause analysis," *Information and Computer Security*, vol. 27, no. 2, hlm. 207–222, 2019, doi: 10.1108/ICS-03-2018-0039.

[27] K. Krombholz, H. Hobel, dan E. Weippl, "Improving security behavior through user training: Experimental evidence," *ACM Transactions on Privacy and Security*, vol. 21, no. 4, hlm. 1–29, 2018, doi: 10.1145/3239551.