AN-NURIYAH
JOURNAL OF ISLAMIC TECHNOLOGY AND INFORMATICS EDUCATION

AN-NURIYAH
Jurnal of Islamic Technology and Informatics Education
Vol. 1 No. 2 Tahun 2025 Page [48-59]

OPEN ACCESS
E-ISSN XXXX-XXXX
P-ISSN XXXX-XXXX

Analisis Keamanan Siber Pada Platform Pendidikan Islam Berbasis Mobile Apps

[1]Miftahul Adila Fitria [2]Hilalludin Hilalludin
[1,2]Universitas Alma Ata Yogyakarta
Email: [1]231100910@almaata.ac.id [2]hilalluddin34@gmail.com

Abstrak
Penelitian ini bertujuan mengidentifikasi bentuk ancaman keamanan siber, memetakan kerentanan yang muncul, serta menganalisis mekanisme perlindungan data yang diterapkan pada platform pendidikan Islam berbasis aplikasi mobile. Penelitian ini juga merumuskan rekomendasi penguatan keamanan berdasarkan temuan literatur. Penelitian menggunakan metode kualitatif deskriptif dengan pendekatan kajian literatur melalui telaah jurnal, laporan keamanan siber, serta regulasi terkait. Hasil kajian menunjukkan bahwa aplikasi pendidikan Islam menghadapi beberapa ancaman utama, seperti kebocoran data pribadi, autentikasi yang lemah, penyalahgunaan API, serta rendahnya standar enkripsi pada proses penyimpanan dan transmisi data. Selain itu, ditemukan bahwa sebagian besar platform belum menerapkan standar keamanan yang konsisten, terutama dalam pengelolaan akses, pengujian kerentanan, dan transparansi kebijakan privasi. Upaya proteksi yang telah dilakukan meliputi penggunaan enkripsi dasar, autentikasi dua langkah, dan sertifikasi protokol keamanan, namun implementasinya masih terbatas pada beberapa platform. Berdasarkan temuan tersebut, penelitian ini merekomendasikan penerapan standar keamanan aplikasi yang lebih ketat, audit keamanan berkala, serta peningkatan literasi digital bagi pengguna dan pengembang untuk memperkuat keandalan platform pendidikan Islam.

Kata kunci: keamanan siber, aplikasi pendidikan Islam, aplikasi mobile, kerentanan digital.

Abstract
This study aims to identify forms of cyber security threats, map emerging vulnerabilities, and analyze data protection mechanisms implemented on mobile application-based Islamic education platforms. This study also formulates recommendations for strengthening security based on literature findings. The research uses a descriptive qualitative method with a literature review approach through journal reviews, cybersecurity reports, and related regulations. The results of the study show that Islamic education applications face several major threats, such as personal data leaks, weak authentication, API abuse, and low encryption standards in data storage and transmission processes. In addition, it was found that most platforms have not implemented consistent security standards, especially in access management, vulnerability testing, and privacy policy transparency. Protection efforts that have been made include the use of basic encryption, two-step authentication, and security protocol certification, but their implementation is still limited to several platforms. Based on these findings, this study recommends the implementation of stricter application security standards, periodic security audits, and increased digital literacy for users and developers to strengthen the reliability of Islamic education platforms.

Keywords: *cybersecurity, Islamic education applications, mobile applications, digital vulnerabilities.*

PENDAHULUAN

Dalam satu dekade terakhir, laju perkembangan teknologi digital telah memicu perubahan besar dalam ranah pendidikan, termasuk pada praktik pendidikan Islam. Penggunaan aplikasi mobile sebagai sarana pembelajaran kini semakin umum karena memberikan fleksibilitas tinggi, kemudahan akses materi, serta ragam fitur interaktif yang mendorong pembelajaran mandiri maupun kegiatan belajar yang terstruktur (H. S. Wibowo, 2023). Fenomena ini juga menunjukkan keselarasan dengan pola belajar generasi saat ini, yang sejak dini telah terbiasa berinteraksi dengan perangkat digital dalam aktivitas harian. Peningkatan pemanfaatan teknologi ini tidak terlepas dari risiko keamanan siber yang semakin beragam, terutama seiring bertambah kompleksnya teknologi digital dan berkembangnya taktik serangan daring (Santoso, 2023). Konteks ini menegaskan bahwa transformasi pendidikan tidak hanya berfokus pada inovasi instruksional, tetapi juga harus memperhatikan aspek perlindungan informasi yang semakin krusial.

Aplikasi pendidikan Islam berbasis mobile umumnya memuat berbagai jenis data sensitif, mulai dari identitas pengguna, rekaman aktivitas pembelajaran, hingga informasi pribadi lain yang bersifat penting. Keberadaan data tersebut menyebabkan platform pendidikan menjadi target yang rentan terhadap beragam ancaman siber, seperti kebocoran data pribadi, akses tanpa izin, penyalahgunaan API, serta kelemahan pada sistem autentikasi dan enkripsi. Ancaman semacam ini tidak hanya dapat mengganggu kelancaran proses belajar, tetapi juga berpotensi meruntuhkan kepercayaan masyarakat terhadap platform pendidikan Islam yang idealnya berfungsi sebagai ruang belajar yang aman dan andal. Oleh karena itu, isu keamanan data pada aplikasi pembelajaran tidak dapat dipandang sebagai permasalahan teknis semata, tetapi sebagai bagian integral dari mutu layanan pendidikan digital.

Perkembangan regulasi mengenai perlindungan data dan keamanan digital termasuk aturan terkait kerahasiaan informasi pribadi serta standar keamanan aplikasi menuntut pengembang platform pendidikan untuk menerapkan langkah pengamanan yang lebih sistematis dan kuat (Pratama et al., 2024). Namun, berbagai studi menunjukkan bahwa implementasi keamanan pada banyak aplikasi pendidikan masih belum konsisten dan kerap tidak memenuhi standar yang direkomendasikan. Beberapa platform diketahui belum menerapkan kebijakan pengelolaan akses yang memadai, kurang optimal dalam melakukan pengujian kerentanan, dan belum transparan dalam menyampaikan kebijakan privasi kepada penggunanya. Kondisi ini menunjukkan adanya jarak antara tuntutan regulatif dan praktik nyata di lapangan, sehingga memerlukan perhatian lebih dari para pemangku kepentingan (Badruddin et al., 2022).

Dengan mempertimbangkan urgensi tersebut, diperlukan sebuah kajian komprehensif yang mampu memetakan berbagai bentuk ancaman siber, menemukan kerentanan yang muncul, serta meninjau kembali mekanisme perlindungan data yang saat ini diterapkan pada aplikasi mobile pendidikan Islam. Pendekatan studi literatur dengan metode deskriptif kualitatif menjadi relevan digunakan karena memungkinkan peneliti untuk mengumpulkan temuan dari jurnal ilmiah, laporan keamanan siber, serta regulasi terkait yang dapat menjelaskan permasalahan ini secara lebih mendalam. Melalui pendekatan tersebut, penelitian diharapkan mampu menghasilkan gambaran yang lebih terstruktur mengenai kondisi aktual keamanan siber pada platform pendidikan Islam dan mengidentifikasi aspek-aspek yang perlu diperkuat dalam pengembangannya.

Dengan demikian, penelitian ini memegang peran penting dalam mendukung terciptanya ekosistem pembelajaran digital yang lebih aman, berkelanjutan, dan responsif terhadap tantangan keamanan informasi di era modern. Temuan penelitian juga diharapkan dapat memberikan kontribusi

bermakna terhadap pengembangan aplikasi pendidikan Islam yang tidak hanya menyediakan materi belajar yang informatif, tetapi juga mengedepankan perlindungan data, kenyamanan, serta rasa aman bagi penggunanya. Upaya ini diharapkan mampu memperkuat kepercayaan publik terhadap platform pembelajaran berbasis teknologi yang semakin dibutuhkan dalam konteks pendidikan masa kini.

METODE PENELITIAN

Penelitian ini menerapkan pendekatan kualitatif deskriptif yang difokuskan pada penelusuran literatur dari berbagai sumber akademik dan praktis, seperti jurnal ilmiah terkini, laporan analisis keamanan siber, serta dokumen regulatif yang mengatur perlindungan data. Pemilihan referensi dilakukan secara bertahap dengan mempertimbangkan tingkat relevansi terhadap topik, validitas ilmiah, serta otoritas lembaga atau penulis yang menerbitkannya. Seluruh informasi yang telah dihimpun kemudian dianalisis melalui proses reduksi data, penyusunan kategori tematik, dan interpretasi deskriptif untuk memperoleh gambaran komprehensif mengenai bentuk ancaman, potensi kerentanan, serta prosedur perlindungan keamanan yang diterapkan pada platform pendidikan Islam berbasis mobile. Melalui analisis tersebut, penelitian ini merumuskan rekomendasi strategis yang bertujuan memperkuat keamanan aplikasi, terutama dalam aspek pengelolaan data pengguna, mitigasi risiko teknis, serta peningkatan kesiapan terhadap insiden keamanan digital (Sugiyono, 2013).

HASIL DAN PEMBAHASAN

Ancaman Keamanan Siber pada Aplikasi Pendidikan Islam

Perkembangan aplikasi pendidikan Islam menawarkan peluang signifikan untuk memperluas akses pembelajaran, namun hal ini dipicu oleh berbagai ancaman keamanan siber yang semakin mendesak di era digital saat ini (Azwar et al., 2024). Tinjauan literatur terkini mengungkapkan bahwa kebocoran data pribadi merupakan risiko utama, khususnya karena platform-

platform tersebut sering mengumpulkan informasi sensitif seperti identitas pengguna, riwayat pembelajaran, dan pola aktivitas akun. Apabila mekanisme perlindungan data tidak dirancang secara menyeluruh, serangan seperti *phishing*, infiltrasi melalui malware, atau pemanfaatan ancaman keamanan dapat terjadi, sehingga berpotensi menyebabkan perlindungan data oleh entitas yang tidak bertanggung jawab (Pardosi et al., 2024). Penerapan autentikasi yang sederhana tanpa enkripsi atau verifikasi multi-lapis meningkatkan risiko pengambilalihan akun, sebuah masalah yang semakin serius seiring dengan maraknya serangan credential stuffing pada platform pendidikan (Mukhlizar & Ikom, 2025).

Ada hal penting lainnya yang berkaitan dengan keamanan antarmuka pemrograman aplikasi (API) yang sering kali diabaikan oleh para pengembang API tanpa perlindungan yang memadai dapat dieksploitasi untuk mengakses atau mengubah data internal secara ilegal (Santoso, 2025). Banyak aplikasi yang belum mengadopsi enkripsi *end to end* dalam penyimpanan dan transmisi data, sehingga membuka kemungkinan intersepsi oleh pihak eksternal (Almadira et al., 2024). Temuan-temuan ini menekankan perlunya penguatan infrastruktur keamanan, implementasi standar perlindungan data, serta peningkatan kesadaran literasi keamanan digital di kalangan pengguna dan pengembang untuk menjaga integritas, privasi, dan keberlanjutan ekosistem pendidikan Islam berbasis digital.

Kerentanan Sistem Keamanan dalam Platform Pendidikan Islam

Sejumlah besar platform pendidikan Islam yang berbasis aplikasi seluler masih dalam tahap permulaan implementasi keamanan digital (Adedo et al., 2024). Kelemahan utama terletak pada pengelolaan akses, di mana alokasi hak pengguna belum sepenuhnya mematuhi prinsip hak istimewa minimal (*least* istimewa), sehingga beberapa peran dasar masih mampu mengakses informasi yang seharusnya dibatasi (Pahleviannur et al., 2022).

Situasi ini memperbesar risiko perubahan data, penghapusan konten, serta mengabaikan fungsi internal. Kurangnya aktivitas pengujian kerentanan, seperti uji penetrasi, audit keamanan, dan pemutakhiran sistem, menyebabkan berbagai celah keamanan tidak teridentifikasi, termasuk pustaka perangkat lunak yang ketinggalan zaman, pengaturan server yang tidak aman, serta sanitasi input yang tidak memadai, yang dapat memicu serangan seperti injeksi SQL, skrip lintas situs, atau eksploitasi pemrograman aplikasi (Rahayu, n.d.).

Kerentanan tambahan muncul dalam kebijakan privasi yang kurang transparan, di mana banyak platform gagal menjelaskan jenis data yang dikumpulkan, metode penyimpanan, jangka waktu retensi, serta tujuan pemrosesan (Tarumingkeng, n.d.). Tidak jelasan ini bertentangan dengan standar perlindungan data pribadi kontemporer dan mengekspos pengguna terhadap risiko dilindungi data untuk tujuan komersial atau pembuatan profil. Absennya prinsip-prinsip seperti minimisasi data, visi tujuan, dan persetujuan yang terinformasi mencerminkan rendahnya kesadaran para pengembang terhadap norma keamanan aplikasi seluler (K. T. Wibowo et al., n.d.). Literatur ini menekankan pentingnya penerapan pengelolaan akses berbasis peran, audit keamanan rutin, serta revisi kebijakan privasi untuk meningkatkan ketahanan dan kepercayaan terhadap platform pendidikan Islam di tengah lanskap digital masa kini.

Mekanisme Perlindungan Keamanan yang Telah Diterapkan

Sejumlah platform pendidikan Islam berbasis aplikasi seluler telah mulai mengadopsi mekanisme perlindungan keamanan dasar, meskipun implementasinya masih bersifat terbatas. Penerapan enkripsi untuk menjaga data sensitif merupakan langkah yang paling sering dilakukan, khususnya melalui protokol SSL/TLS yang bertujuan mengamankan pertukaran data antara perangkat pengguna dan server (Ramadhani et al., 2025). Beberapa

aplikasi juga telah menggabungkan autentikasi dua faktor untuk meningkatkan keamanan proses masuk dan meminimalkan risiko pencurian akun, sebuah strategi yang semakin penting seiring dengan maraknya serangan kredensial di bidang pendidikan digital (Abdullah et al., 2025). Penerapan teknik *hashing* dan penyimpanan terenkripsi untuk kata sandi mulai diterapkan oleh beberapa platform, yang menunjukkan peningkatan kesadaran terhadap praktik lisensi yang lebih aman (Puspitaningrum & Insani, 2024).

Namun mekanisme implementasi ini belum sepenuhnya terintegrasi dan belum mencakup semua elemen keamanan yang diperlukan oleh aplikasi pendidikan Islam (Rojak, 2024). Banyak platform yang belum dilengkapinya dengan kontrol akses internal yang ketat, pencatatan log aktivitas, atau pemantauan anomali secara langsung. Absennya lapisan keamanan tambahan ini menyebabkan upaya proteksi yang ada belum mampu memberikan perlindungan komprehensif terhadap ancaman serangan yang semakin canggih (Aska et al., 2024). Dalam konteks aplikasi yang mengelola data keagamaan, identitas siswa dan pengajar, serta rekam jejak jejak lembaga pendidikan Islam, perlindungan yang sebagian tidak cukup untuk memastikan keamanan dan privasi pengguna (Francis et al., 2023). Tantangan ini menyoroti kebutuhan akan pendekatan keamanan yang lebih menyeluruh, meliputi penerapan standar keamanan aplikasi terkini, otomatisasi pemantauan, dan peningkatan kapasitas pengembang dalam mengatasi evolusi ancaman siber masa kini (diat et al., 2024).

Analisis Kebutuhan Penguatan Keamanan

Penguatan keamanan siber pada platform pendidikan Islam berbasis aplikasi seluler merupakan prioritas yang sangat mendesak. Ancaman digital yang semakin canggih mengharuskan diterapkannya standar keamanan yang lebih ketat guna menjamin perlindungan komprehensif terhadap data sensitif

(Buana & Kurniawan, 2023). Enkripsi menyeluruh, meliputi enkripsi *end to end*, diperlukan untuk memastikan data tetap aman di semua tahap pengiriman. Mekanisme autentikasi multilapis diperlukan untuk mengurangi risiko pengambilalihan akun melalui enkripsi kredensial (Tompul & others, 2024). Sistem deteksi intrusi dan pemantauan aktivitas secara *real time* diperlukan untuk mendeteksi pola akses yang mencurigakan yang mungkin menunjukkan upaya infiltrasi.

Audit keamanan rutin diperlukan untuk memverifikasi bahwa kerentanan dapat diidentifikasi dan diperbaiki sebelum dieksploitasi oleh entitas yang tidak sah (Izzati & Kasmawi, 2024). Evaluasi arsitektur keamanan, pengujian kerentanan, dan peninjauan kebijakan data merupakan bagian integral dari proses penguatan ini. Kebijakan privasi yang transparan, konsisten, dan informatif diperlukan agar pengguna memahami mekanisme pengumpulan, penyimpanan, dan pemanfaatan data mereka (Zaeem et al., 2020). Transparansi dalam pengelolaan data diperlukan untuk membangun kepercayaan masyarakat terhadap platform pendidikan Islam.

Literasi digital pengguna juga merupakan komponen krusial dalam penguatan keamanan. Penggunaan kata sandi yang lemah, kebiasaan berbagi akun, dan pengabaian protokol keamanan menjadi faktor risiko yang dapat memicu kerentanan sistem. Pendidikan keamanan informasi bagi siswa, pengajar, dan administrator lembaga pendidikan diperlukan untuk meminimalkan risiko yang berasal dari perilaku pengguna (Park & Chung, 2022).

KESIMPULAN

Kajian mengenai keamanan siber pada platform pendidikan Islam berbasis aplikasi seluler mengungkapkan bahwa ekosistem pembelajaran digital ini masih merupakan ancaman yang substansial, khususnya berkaitan dengan kebocoran data pribadi, autentikasi yang tidak memadai, pengontrol

antarmuka pemrograman aplikasi, serta standar enkripsi yang belum optimal. Kerentanan sistem teridentifikasi melalui pengelolaan akses yang lemah, melemahkan aktivitas pengujian kerentanan, dan tidak transparanan dalam kebijakan privasi, yang pada gilirannya meningkatkan risiko eksploitasi oleh aktor kejahatan siber. Meskipun sejumlah mekanisme perlindungan seperti enkripsi dasar, autentikasi dua faktor, dan sertifikasi protokol telah diimplementasikan, penerapannya belum merata dan belum memenuhi tuntutan perlindungan data yang semakin kompleks.

Penguatan keamanan harus dilakukan melalui penerapan enkripsi menyeluruh, autentikasi multilapis, audit keamanan rutin, serta peningkatan transparansi dalam pengelolaan data. Literasi digital pengguna juga diperlukan untuk mengurangi risiko yang timbul dari perilaku pengguna itu sendiri. Temuan-temuan ini menegaskan bahwa platform pengembangan pendidikan Islam yang aman dan dapat dipercaya memerlukan pendekatan teknis, manajerial, dan edukatif yang terintegrasi secara harmonis.

DAFTAR PUSTAKA

Abdullah, S., Widyastuti, T. A. R., Suharyanto, C. E., Januru, L., Safii, M., Santioso, L. L., Aldin, M., & Faqihuddin, A. (2025). *Pemberdayaan Media Cyber Di Era Digital*. Yayasan Tri Edukasi Ilmiah.

Adedo, E., Deriwanto, D., & Others. (2024). *Perkembangan Media Digital Dan Pemanfaatannya Dalam Pembelajaran Pendidikan Agama Islam*. Institut Agama Islam Negeri Curup.

Almadira, A., Pratama, Y., & Purwani, F. (2024). Melindungi Data Di Dunia Digital: Peran Stategis Enkripsi Dalam Keamanan Data. *Journal Of Scientech Research And Development*, *6*(2), 540–549.

Aska, M. F., Putra, D. P., & Sinambela, C. J. M. (2024). Strategi Efektif Untuk Implementasi Keamanan Siber Di Era Digital. *Journal Of Informatic And Information Security*, *5*(2), 187–200.

Azwar, I., Inayah, S., Nurlela, L., Kania, N., Kusumaningrum, B., Prasetyaningrum, D. I., Kau, M. S., Lestari, I., & Permana, R. (2024). *Pendidikan Di Era Digital*.

Badruddin, S., Halim, P., Ismowati, M., & Others. (2022). *Transformasi Digital Dalam Pelayanan Publik*. Zahir Publishing.

Buana, R. A., & Kurniawan, Y. (2023). Pengujian Keamanan Aplikasi Mobile Learning Management System Berbasis Deep Reinforcement Learning Dengan Model Fuzzing Adaptif. *Jurnal Pendidikan Dan Teknologi Indonesia*. Https://Doi.Org/10.52436/1.Jpti.957

Diat, S., Kurniawan, H., & Nugroho, C. (2024). Pengembangan Sistem Informasi Penilaian Keamanan Aplikasi Berdasarkan Application Security Verification Standard (Asvs). *Indexia : Informatics And Computational Intelligent Journal*, *6*(1), 62–71. Https://Doi.Org/10.30587/Indexia.V6i1.7629

Francis, M., Avoseh, M. B. M., Card, K., Newland, L., & Streff, K. (2023). Student Privacy And Learning Analytics: Investigating The Application Of Privacy Within A Student Success Information System In Higher Education. *Journal Of Learning Analytics*, *10*(3), 102–114. Https://Doi.Org/10.18608/Jla.2023.7975

Izzati, P. N., & Kasmawi, K. (2024). Static Analysis-Based Security Enhancement For Mobile Applications Using Mobile Security Framework (Mobsf). *Journal Of Applied Informatics And Computing*, *9*(4), [–]-[–]. Https://Doi.Org/10.30871/Jaic.V9i4.9525

Mukhlizar, S. A., & Ikom, M. (2025). Etika Masyarakat Digital. *Etika Masyarakat Digital*, 30.

Pahleviannur, M. R., De Grave, A., Saputra, D. N., Mardianto, D., Hafrida, L., Bano, V. O., Susanto, E. E., Mahardhani, A. J., Alam, M. D. S., Lisya, M., & Others. (2022). *Metodologi Penelitian Kualitatif*. Pradina Pustaka.

Pardosi, V. B. A., Deta, B., Nugroho, F., & Vandika, A. Y. (2024). *Sistem Keamanan Informasi*.

Park, Y. J., & Chung, J. (2022). Examining Digital Literacy And Privacy Behavior Of Internet Users. *Telematics And Informatics*, *65*, 101732. Https://Doi.Org/10.1016/J.Tele.2021.101732

Pratama, A. M., Syaiful, M., & Rahman, M. F. (2024). *Keamanan Data Dan Informasi*. Kaizen Media Publishing.

Puspitaningrum, N., & Insani, K. T. K. C. (2024). Kesadaran Akan Keamanan Digital. *Transformasi Pembelajaran Anak Usia Dini Di Zaman Digital*, 116.

Rahayu, S. K. (N.D.). *Keamanan Digital Dalam Audit Pajak. Integrasi Cyber Security Dengan Crm, Bda, Dan Bi Untuk Revolusi Compliance*.

Ramadhani, M., Todi, Y. A., Hidayat, R., & Others. (2025). Komparasi Hukum Indonesia Dan Hukum Islam Terhadap Perlindungan Data Pribadi Dalam Transaksi Ekonomi Syariah Digital. *Jurnal Media Akademik (Jma)*, *3*(4).

Rojak, J. A. (2024). Penerapan Nilai-Nilai Islam Dalam Pendidikan Modern: Tantangan Dan Strategi Efektif. *Jurnal Pendidikan, Penelitian, Dan Pengabdian Masyarakat*, *4*(2), 18–34.

Santoso, J. T. (2023). Teknologi Keamanan Siber (Cyber Security). *Penerbit Yayasan Prima Agus Teknik*, 1–173.

Santoso, J. T. (2025). Desain Dan Implementasi Api Untuk Cloud Computing Dengan Azure Dan Aws. *Penerbit Yayasan Prima Agus Teknik*.

Sugiyono, D. (2013). *Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif Dan R\&D*.

Tarumingkeng, R. C. (N.D.). *Manajemen Siber*.

Tompul, F. B., & Others. (2024). *Analisis Keamanan Sistem Informasi Berbasis Web Menggunakan Teknologi Enkripsi End-To-End*. Universitas Labuhanbatu.

Wibowo, H. S. (2023). *Pengembangan Teknologi Media Pembelajaran: Merancang Pengalaman Pembelajaran Yang Inovatif Dan Efektif*. Tiram Media.

Wibowo, K. T., Sh, M. H., Dj, M. A., Mh, D. A. K., St, M. M., Abdul Karim, S. H., Mi, K., Rizki Syafril, S. H. I., Ma'Rifah, S. H., & Mh, D. H. M. (N.D.). *Hukum Digital Dan Privasi Data*.

Zaeem, R. N., Puschell, J., & Reddy, Z. L. (2020). Privacy Policies And Transparency In Mobile Applications. *Empirical Software Engineering*, *25*(6), 1–34. Https://Doi.Org/10.1007/S10664-020-09833-1