Social, Humanities, and Educational Studies

SHEs: Conference Series 8 (4) (2025) 932 – 939

Implementasi Algoritma Kriptografi AES-128, Base 64 Dan Hashing Bcrypt Dalam Mengamankan Pesan Rahasia Berbasis Android

Gunawan, Wahyu Albara, Harry Witriyono, Muhammad Imanullah

Universitas Muhammadiyah Bengkulu
gunawan@umb.ac.id

Article History
accepted 1/11/2025 approved 1/12/2025 published 29/12/2025

Abstract
Data security is a crucial necessity in digital communication, particularly on mobile devices which are vulnerable to information leaks and privacy breaches. This research addresses the gap by testing the comprehensive integration of three data security methods within a single Android application: AES-128 cryptography (for confidentiality), Base64 encoding (for transmission compatibility), and Bcrypt hashing (for integrity). The research methodology utilizes a Waterfall-based software engineering approach and involves simulated performance testing of the algorithms on text messages. The novelty of this study lies in the integrated performance analysis of the three algorithms on resource-constrained mobile platforms. The results show that this integration operates with 100% accuracy in encryption-decryption scenarios. Specifically, AES-128 successfully maintained an average processing speed of under 50 milliseconds per transaction, and Bcrypt was proven to generate unique and rainbow table-resistant hashes. It is concluded that this application is capable of protecting messages from unauthorized access and serves as a practical and efficient solution for enhancing digital communication privacy on the Android platform. This research provides a tangible contribution in the form of a measurable end-to-end security implementation model for the Android platform.
Keywords: *AES-128, Android Base64, Bcrypt, Cryptography, Message Security*

Abstrak
Keamanan data merupakan kebutuhan krusial dalam komunikasi digital, terutama pada perangkat mobile yang rentan terhadap kebocoran dan pelanggaran privasi. Penelitian ini mengatasi gap dengan menguji integrasi komprehensif tiga metode pengamanan data dalam satu aplikasi Android: kriptografi AES-128 (untuk kerahasiaan), encoding Base64 (untuk kompatibilitas transmisi), dan hashing Bcrypt (untuk integritas). Metodologi penelitian menggunakan pendekatan rekayasa perangkat lunak berbasis Waterfall dan melibatkan pengujian performa algoritma secara simulatif pada pesan teks. Novelty penelitian ini terletak pada analisis kinerja terpadu ketiga algoritma pada platform mobile berdaya terbatas. Hasil penelitian menunjukkan bahwa integrasi ini bekerja secara 100% akurat dalam skenario enkripsi-dekripsi. Secara spesifik, AES-128 berhasil mempertahankan kecepatan pemrosesan rata-rata di bawah 50 milidetik per transaksi, dan Bcrypt terbukti menghasilkan hash yang unik dan tahan rainbow table. Disimpulkan bahwa aplikasi ini mampu melindungi pesan dari akses tidak sah serta menjadi solusi praktis dan efisien dalam meningkatkan privasi komunikasi digital. Penelitian ini memberikan kontribusi nyata berupa model implementasi end-to-end security yang terukur pada platform Android.
Kata kunci: *AES-128, Android ,Base64, Bcrypt, Keamanan Pesan, Kriptografi,*

Social, Humanities, and Education Studies (SHEs): Conference Series p-ISSN 2620-9284
https://jurnal.uns.ac.id/shes e-ISSN 2620-9292

PENDAHULUAN

Perkembangan teknologi informasi yang begitu pesat pada era digital telah membawa perubahan signifikan dalam berbagai sektor kehidupan manusia. Kemajuan dalam bidang pendidikan, industri, komunikasi, hingga layanan publik tidak terlepas dari peran teknologi digital yang mempermudah akses terhadap informasi serta meningkatkan efektivitas dan efisiensi berbagai aktivitas (OECD, 2021). Internet, kecerdasan buatan, komputasi awan, dan perangkat mobile kini menjadi bagian tak terpisahkan dari kehidupan sehari-hari (World Economic Forum, 2023). Kemudahan yang ditawarkan teknologi ini mendorong masyarakat untuk terus beradaptasi agar mampu mengikuti perkembangan zaman, sehingga teknologi tidak hanya berfungsi sebagai alat bantu, tetapi juga sebagai pondasi penting bagi peningkatan kualitas peradaban manusia (United Nations, 2020).

Salah satu bidang yang mengalami perkembangan paling pesat adalah komunikasi digital. Kemajuan jaringan komputer dan teknologi komunikasi telah memungkinkan jutaan orang saling terhubung melalui berbagai platform pesan instan, media sosial, maupun aplikasi berbasis cloud (Kemp, 2023). Interaksi jarak jauh kini dapat dilakukan secara real time menggunakan perangkat yang semakin ringkas namun bertenaga. Meskipun demikian, kemajuan tersebut juga menghadirkan tantangan baru, terutama pada aspek keamanan data dan privasi pengguna. Bahkan, laporan statistik global menunjukkan bahwa insiden kebocoran data yang melibatkan platform komunikasi dan messaging telah meningkat lebih dari 35% pada tahun 2023, di mana jutaan record informasi sensitif pengguna terekspos (Cybersecurity Ventures, 2024). Risiko seperti penyadapan, pencurian identitas, manipulasi data, serta penyebaran informasi sensitif oleh pihak tidak bertanggung jawab menjadi ancaman yang semakin nyata di era keterhubungan digital.

Dalam konteks inilah keamanan data menjadi kebutuhan yang tidak dapat diabaikan. Setiap data yang ditransmisikan melalui jaringan memiliki potensi untuk diakses atau disalahgunakan oleh pihak ketiga jika tidak dilindungi dengan mekanisme yang memadai. Oleh karena itu, berbagai upaya pengamanan, baik dari sisi perangkat keras, perangkat lunak, maupun protokol komunikasi, diperlukan untuk menjamin kerahasiaan, integritas, dan autentikasi data. Salah satu mekanisme yang paling banyak digunakan dalam sistem keamanan digital adalah teknik kriptografi. Kriptografi, yang secara etimologis berasal dari bahasa Yunani yang berarti 'tulisan tersembunyi', adalah studi tentang teknik matematika untuk mengamankan komunikasi (Amin, 2020). Secara esensial, teknik ini digunakan dalam aplikasi pesan pada perangkat Android untuk tiga fungsi utama: menjamin kerahasiaan dengan memastikan hanya pihak yang dituju yang dapat membaca pesan; menjaga integritas dengan memastikan pesan tidak diubah selama transmisi; dan melakukan autentikasi untuk memverifikasi identitas pengguna serta keaslian pesan yang dikirimkan.

Dalam proses komunikasi digital, data asli yang belum disandikan disebut plaintext, yang setelah dienkripsi menggunakan algoritma akan berubah menjadi ciphertext, yaitu bentuk tersamar yang tidak dapat dipahami tanpa kunci dekripsi. Meskipun algoritma kriptografi klasik (seperti yang diteliti oleh Eril Obeit Choiri (2020)) telah membuktikan kemampuan dasar dalam menjaga kerahasiaan data selama transmisi, kompleksitas dan volume data pada aplikasi pesan mobile modern membutuhkan standar keamanan yang jauh lebih tinggi. Oleh karena itu, sistem keamanan saat ini harus mengimplementasikan algoritma kriptografi modern yang efisien dan kuat, seperti AES (untuk enkripsi data), Base64 (untuk memastikan data biner aman ditransmisikan melalui teks), dan Bcrypt (khusus untuk pengamanan password), guna menjamin pertahanan terhadap ancaman siber kontemporer.

Seiring berkembangnya teknologi, kebutuhan akan algoritma kriptografi yang lebih kuat dan efisien semakin meningkat. Kriptografi modern menawarkan tingkat

keamanan yang jauh lebih tinggi melalui algoritma yang berbasis operasi matematis kompleks, salah satunya adalah Advanced Encryption Standard (AES). Dalam konteks pengamanan data pada perangkat mobile, AES-128 sering digunakan karena sifatnya yang ringan namun tetap memberikan keamanan yang kuat. AES-128 merupakan algoritma enkripsi simetris yang mengubah plaintext menjadi ciphertext dengan menggunakan kunci privat. Keunggulannya terletak pada efisiensi pemrosesan sehingga sangat cocok diterapkan pada perangkat seperti smartphone yang memiliki keterbatasan daya dan kapasitas pemrosesan. Pemilihan AES-128 didasarkan pada alasan yang kuat, yaitu menawarkan kecepatan enkripsi dan dekripsi yang superior dibandingkan cipher lain dengan panjang kunci yang sama, serta memiliki kebutuhan memori (footprint) yang minimal (Rinaldi, 2022). Lebih lanjut, AES-128 merupakan standar yang direkomendasikan oleh NIST dan banyak digunakan sebagai primitive kriptografi dalam protokol keamanan mobile (Schneier & Ferguson, 2021), menjadikannya pilihan ideal untuk platform Android guna menjamin keamanan data tanpa mengorbankan kinerja atau daya baterai perangkat.

Selain enkripsi, mekanisme encoding seperti Base64 juga diperlukan dalam proses pengiriman data digital. Base64 memungkinkan ciphertext dikonversi ke dalam format teks ASCII sehingga kompatibel dengan berbagai protokol komunikasi yang hanya mendukung karakter tertentu. Meskipun Base64 tidak bersifat sebagai mekanisme keamanan, teknik ini berfungsi memastikan bahwa data terenkripsi dapat ditransmisikan tanpa mengalami kerusakan format.

Dalam aspek autentikasi dan perlindungan kata sandi, hashing Bcrypt menjadi salah satu metode yang paling direkomendasikan. Bcrypt dirancang untuk tahan terhadap serangan brute force dengan melakukan proses hashing berulang (work factor) yang memerlukan waktu komputasi lebih lama dibandingkan algoritma hashing konvensional. Penggunaan Bcrypt secara signifikan meningkatkan keamanan autentikasi pengguna karena hasil hashing tidak dapat dibalik dan sulit untuk diretas menggunakan metode komputasi modern. Menurut penelitian Al Farissi, Arya Pradata, dan Kanda Miraswan (2020), kombinasi metode AES-128, Base64, dan Bcrypt terbukti mampu meningkatkan tingkat keamanan data digital, terutama dalam aplikasi yang berjalan pada perangkat bergerak.

Meskipun demikian, implementasi beberapa teknik keamanan secara bersamaan pada aplikasi mobile memiliki tantangan tersendiri, seperti kebutuhan optimasi performa agar proses enkripsi, encoding, dan hashing tidak membebani perangkat secara berlebihan. Pengembang perlu mempertimbangkan efisiensi algoritma, manajemen memori, serta pengalaman pengguna agar aplikasi tetap responsif dan mudah digunakan.

Berdasarkan fenomena peningkatan ancaman siber pada komunikasi digital dan adanya gap penelitian di mana studi sebelumnya cenderung berfokus pada implementasi algoritma kriptografi secara tunggal (sehingga kurang optimal untuk keamanan berlapis), penelitian ini bertujuan mengisi kekosongan tersebut. Oleh karena itu, rumusan masalah utama adalah bagaimana merancang, mengimplementasikan, dan mengevaluasi kinerja serta tingkat keamanan integrasi komprehensif dari algoritma AES-128, encoding Base64, dan hashing Bcrypt dalam satu aplikasi mobile berbasis Android untuk meningkatkan keamanan pesan digital. Tujuan penelitian ini terbagi tiga: pertama, mengembangkan aplikasi Android yang mengamankan pesan melalui ketiga metode tersebut secara terpadu; kedua, menguji dan menganalisis performa kecepatan proses enkripsi/dekripsi AES-128 dan hashing Bcrypt pada platform Android; dan ketiga, mengevaluasi efektivitas dan keamanan kombinasi metode ini dalam menjaga kerahasiaan, integritas, dan autentikasi data.

Kontribusi khusus dan kebaruan penelitian ini terletak pada penyajian model integrasi end-to-end yang unik dan komprehensif dari tiga fungsi keamanan (encryption, encoding, dan hashing) dalam satu aplikasi Android. Kontribusi ini diperkuat dengan penyediaan data empiris mengenai kinerja dan overhead waktu pemrosesan algoritma AES-128 dan Bcrypt pada perangkat mobile berdaya terbatas. Hasil penelitian ini diharapkan dapat menjadi referensi teknis yang kuat dalam pengembangan aplikasi keamanan digital, khususnya untuk pengamanan pesan instan di platform Android.

METODE

Penelitian ini menggunakan pendekatan rekayasa perangkat lunak berbasis model Waterfall karena spesifikasi sistem telah ditetapkan sejak awal. Implementasi difokuskan pada pengujian algoritma keamanan data pada aplikasi Android yang dikembangkan menggunakan teknologi cross-platform dengan bahasa pemrograman utama JavaScript melalui framework Vue.Js dan Ionic/Capacitor. Lingkungan pengembangan utama yang digunakan adalah Visual Studio Code, dengan Android Build Tools v33.0.0 sebagai target platform. Untuk fungsionalitas kriptografi, proyek ini mengintegrasikan dua pustaka spesifik: Crypto.js (misalnya, v4.1.1) untuk implementasi AES-128 dan bcrypt.js (misalnya, v2.4.0) untuk hashing yang aman. Tahapan penelitian mencakup analisis kebutuhan, perancangan (flowchart integrasi algoritma), pengkodean, pengujian, dan implementasi, dengan pengujian dilakukan pada emulator NoxPlayer (atau perangkat fisik yang ditentukan). Data penelitian mencakup data konseptual (literatur teknis) dan data eksperimental berupa pesan teks dengan variasi panjang karakter (misalnya 10, 50, dan 100 karakter). Analisis data dilakukan secara fungsional dan komparatif, berfokus pada analisis teknis integrasi di mana plaintext dienkripsi AES-128, di-encode Base64 untuk transmisi, dan key derivation atau metadata diamankan menggunakan Bcrypt, sekaligus mengukur performa waktu pemrosesan algoritma (dalam milidetik).

HASIL DAN PEMBAHASAN

Pengembangan sistem keamanan data dalam aplikasi mobile berbasis Android menuntut penerapan algoritma kriptografi modern yang tidak hanya kuat secara matematis, tetapi juga efisien dan mudah diimplementasikan. Dalam penelitian ini, dua pustaka kriptografi berbasis JavaScript Crypto.js dan bcrypt.js diintegrasikan untuk memenuhi kebutuhan enkripsi simetris dan hashing satu arah. Secara teknis, integrasi ini membentuk pipeline keamanan: data pesan dienkripsi oleh Crypto.js (menggunakan AES), sementara bcrypt.js berperan sebagai mekanisme hashing yang tidak dapat dibalik, diutamakan untuk mengamankan kunci sesi atau metadata sensitif lainnya. Integrasi kedua pustaka ini membentuk fondasi sistem keamanan yang lebih komprehensif, mendukung perlindungan data mulai dari level pengguna hingga level sistem, dan memfasilitasi end-to-end security dalam ekosistem mobile.

AES-128 yang diimplementasikan melalui Crypto.js dipilih karena sifatnya yang cepat, aman, dan telah lama menjadi standar internasional dalam perlindungan data digital. Menurut Alaba dan Li (2021), AES tetap menjadi algoritma simetris paling stabil dan efisien untuk platform mobile karena kemampuannya menangani blok data dengan performa kecepatan tinggi (diukur dalam milidetik) dan ketahanannya terhadap serangan brute force maupun teknik analisis kriptografis modern. Pada proses enkripsi, pesan pengguna diubah menjadi ciphertext menggunakan kunci 128-bit, kemudian dikodekan ke Base64 agar hasilnya aman dan kompatibel untuk transmisi protokol berbasis teks dan display antarmuka. Visualisasi hasil konkret menunjukkan bahwa ciphertext yang dihasilkan selalu berbeda untuk setiap kunci unik, menjamin kerahasiaan. Proses dekripsi dilakukan dengan kunci yang sama sehingga ciphertext dapat dikembalikan ke bentuk asli secara konsisten, menjadikan model kerja ini mudah

diterapkan dan dipahami oleh pengguna, sekaligus meminimalkan latency dalam komunikasi real-time.

Di sisi lain, bcrypt.js bekerja berdasarkan prinsip hashing satu arah dengan penggunaan salt otomatis yang menghasilkan keluaran unik pada setiap proses hashing, bahkan untuk input yang sama. Menurut Pereira dan Souza (2022), bcrypt masih menjadi salah satu algoritma hashing paling direkomendasikan untuk pengamanan kredensial karena ketahanannya terhadap serangan brute force dan rainbow table. Analisis keamanan menunjukkan bahwa mekanisme salt internal dan cost factor yang dapat diatur memberikan ketahanan yang jauh lebih tinggi dibandingkan hash cepat lainnya (seperti MD5 atau SHA-256) dalam konteks pengamanan password pengguna Android. Integrasi bcrypt dalam sistem ini juga mendukung aspek manajemen kunci, di mana key derivation dari kata sandi pengguna dapat diamankan sebelum digunakan untuk proses enkripsi AES. Hal ini menjamin bahwa data sensitif pengguna tidak akan pernah bisa dikembalikan ke bentuk aslinya, sehingga tingkat keamanan meningkat secara signifikan, khususnya dalam konteks aplikasi mobile yang memerlukan autentikasi.

Antarmuka aplikasi dirancang sederhana dan intuitif dengan menyediakan kolom input pesan, tombol untuk enkripsi, dekripsi, dan hashing, serta area tampilan hasil. Struktur antarmuka ini menunjukkan bahwa sistem diarahkan agar dapat digunakan oleh pengguna umum tanpa harus memahami konsep kriptografi secara mendalam. Contoh hasil konkret yang ditampilkan pada antarmuka mencakup waktu pemrosesan (performa) untuk enkripsi/dekripsi sebuah pesan, menampilkan plaintext, ciphertext, dan hash Bcrypt yang dihasilkan. Aplikasi juga dilengkapi dengan fitur riwayat enkripsi yang menyimpan pesan asli, hasil enkripsi AES, hasil dekripsi, serta waktu proses. Fitur riwayat ini memperkuat aspek transparansi dan auditabilitas proses teknis, sehingga pengguna dapat meninjau kembali hasil yang telah dilakukan. Sebagaimana dicatat oleh Ramadhani dan Suhartono (2020), sistem kriptografi yang baik tidak hanya aman tetapi juga menyediakan kemampuan verifikasi proses untuk memastikan integritas data.

Selain fitur enkripsi dasar, aplikasi ini dilengkapi dengan menu “Enkripsi + Generate Key” yang memungkinkan pengguna memasukkan kunci secara manual atau menghasilkan kunci acak sepanjang 16 karakter untuk memenuhi standar AES-128. Mekanisme generate key otomatis ini sangat penting karena mencegah pengguna membuat kunci yang mudah ditebak. Pendekatan ini sesuai dengan rekomendasi Mahendra (2021), yang menekankan bahwa sistem keamanan data pada aplikasi mobile harus menyediakan mekanisme manajemen kunci yang dapat meminimalkan kesalahan pengguna tanpa mengurangi fleksibilitas. Dengan demikian, keamanan sistem dapat meningkat tanpa menuntut pengguna memiliki pemahaman teknis yang tinggi. Adapun hasil pengujian sistem dapat dilihat dalam Tabel berikut:

Tabel 1. Hasil pengujian sistem

No	Skenario Pengujian	Data Uji	Target yang Diharapkan	Hasil Uji	Validasi
1	Pengujian enkripsi pesan	Pesan: Data Rahasia	Sistem menghasilkan ciphertext (teks terenkripsi) yang tidak bisa dibaca secara langsung	Ciphertext muncul dan tidak dapat dibaca	Valid
2	Pengujian dekripsi pesan	Ciphertext dari No.1	Sistem berhasil mengembalikan ciphertext menjadi Data Rahasia	Plaintext kembali ke Data Rahasia	Valid
3	Enkripsi dengan karakter khusus	Pesan: Universitas Muhammadiyah Bengkulu	Ciphertext tetap terbentuk walaupun input mengandung karakter khusus	Ciphertext terbentuk dengan karakter acak	Valid
4	Dekripsi karakter khusus	Ciphertext dari No.3	Sistem berhasil mengembalikan teks ke Universitas Muhammadiyah Bengkulu	Plaintext kembali sesuai karakter awal	Valid

5	Enkripsi dengan input kosong	Pesan kosong	Sistem menampilkan pesan kesalahan atau tidak memproses	Muncul pesan error Input tidak boleh kosong	Valid
6	Dekripsi data yang bukan hasil enkripsi	Input acak ABC123	Sistem menolak atau menampilkan error	Muncul pesan error Format tidak dikenali	Valid

Pengujian sistem dilakukan menggunakan pendekatan blackbox testing untuk memastikan fungsionalitas tanpa meninjau struktur internal program. Hasil pengujian menunjukkan bahwa AES-128 dapat mengembalikan ciphertext menjadi plaintext dengan akurat selama kunci yang digunakan benar, menandakan stabilitas implementasi Crypto.js. Pada sisi lain, sifat satu arah bcrypt terbukti konsisten karena setiap proses hashing menghasilkan keluaran berbeda meskipun input sama, mengonfirmasi integritas mekanisme salt. Pengujian waktu eksekusi juga dilakukan untuk menilai performa algoritma. Hasilnya menunjukkan bahwa waktu eksekusi rata-rata berada di kisaran 1 ms untuk pesan pendek dan sekitar 2,5 ms untuk pesan panjang, sehingga kombinasi AES-128 dan Base64 dinilai tetap responsif dan efisien untuk perangkat mobile. Temuan ini konsisten dengan Pradata dan Miraswan (2020) yang menyatakan bahwa AES dan Base64 memiliki performa optimal pada perangkat mobile karena kompleksitas hitung yang lebih rendah dibanding algoritma simetris lainnya seperti TripleDES.

Tabel 2. Hasil Pengujian Aes 128 + Base64

Panjang Pesan	Base64 Encode(ms)	AES-128 Encrypt (ms)	Base64 Decode (ms)	Aes-128 Decrypt (ms)	Total (ms)
10	0.037880	0.580	0.039540	0.375	1.033
100	0.029960	0.172	0.031360	0.195	0.428
500	0.219960	0.724	0.042580	0.726	1.713
1000	0.177620	1.445	0.079580	0.825	2.527
5000	1.407200	0.944	1.266460	2.034	5.652

Jika dibandingkan dengan penelitian sebelumnya, temuan penelitian ini memiliki kesesuaian kuat. Widodo dan Hartati (2021) menemukan bahwa implementasi AES-128 pada aplikasi mobile menghasilkan kinerja tinggi dan tingkat keamanan yang stabil, bahkan pada variasi panjang pesan yang signifikan. Hal serupa juga terlihat pada penelitian Sari dan Mulia (2020), yang membandingkan bcrypt dengan SHA-256 untuk kebutuhan autentikasi. Hasil penelitian mereka menunjukkan bahwa bcrypt lebih unggul karena salt otomatis dan cost factor yang dapat disesuaikan, menjadikannya lebih aman dalam mencegah serangan brute force. Keselarasan ini memperkuat alasan penggunaan bcrypt dalam sistem yang dikembangkan pada penelitian ini.

Secara keseluruhan, dukungan teori para ahli, hasil penelitian terdahulu, dan temuan pengujian menunjukkan bahwa integrasi Crypto.js dan bcrypt.js merupakan pendekatan yang kuat dan efisien dalam membangun sistem keamanan data pada aplikasi mobile berbasis Android. AES-128 memberikan perlindungan tingkat tinggi pada enkripsi simetris, sementara bcrypt memastikan keamanan optimal dalam proses hashing. Antarmuka yang mudah digunakan, fitur riwayat enkripsi, serta mekanisme generate key memberikan nilai tambah dari sisi penggunaan praktis. Oleh karena itu, sistem keamanan data yang dikembangkan dalam penelitian ini dapat menjadi rujukan

penting bagi pengembangan aplikasi mobile modern yang membutuhkan keseimbangan antara keamanan, performa, dan kemudahan penggunaan.

SIMPULAN

Berdasarkan hasil penelitian dan implementasi yang telah dilakukan, dapat disimpulkan bahwa penerapan algoritma kriptografi modern pada fitur aplikasi Android telah berhasil dilakukan secara terintegrasi dan efektif. Secara spesifik, algoritma AES-128 berhasil melakukan proses enkripsi dan dekripsi pesan pada seluruh (100%) skenario uji coba dengan akurasi dan konsistensi data yang sempurna. Selain itu, penerapan hashing Bcrypt pada ciphertext telah terbukti menghasilkan hash yang unik dan berbeda pada setiap eksekusi, bahkan ketika input pesan yang sama digunakan, sehingga secara efektif menjamin integritas data dan mencegah serangan rainbow table. Sementara itu, Base64 memastikan kompatibilitas data terenkripsi untuk transmisi melalui protokol berbasis teks. Dengan penerapan ketiga metode tersebut pada fitur berbeda namun saling melengkapi, aplikasi Android yang dikembangkan berhasil mengamankan pesan rahasia secara efektif, baik dari sisi kerahasiaan, kompatibilitas data, maupun keutuhan informasi. Penelitian selanjutnya disarankan untuk mengevaluasi dan membandingkan performa algoritma AES-128 dengan algoritma kriptografi lain, seperti RSA atau ChaCha20, untuk mendapatkan pendekatan yang lebih optimal dari sisi kecepatan dan keamanan. Aplikasi dapat dikembangkan lebih lanjut agar mendukung pengamanan jenis pesan lain, seperti gambar, video, atau dokumen, dengan metode kriptografi yang sesuai. Pengembangan sistem keamanan lebih lanjut dapat dilakukan dengan menambahkan lapisan keamanan tambahan.

DAFTAR PUSTAKA

Al Farissi, M., Pradata, A., & Miraswan, K. (2020). Analisis keamanan kombinasi AES-128, Base64, dan Bcrypt pada platform mobile. *Jurnal Sistem Informasi dan Teknologi, 12*(1), 55–63.

Alaba, O., & Li, Q. (2021). Evaluating the efficiency of AES encryption on mobile computing platforms. *Journal of Mobile Security and Applications*, 9(2), 112–124.

Amin, M. (2020). *Kriptografi dan keamanan informasi*. Jakarta: Penerbit Informatika.

Aryanto, M. B., Tahir, M., Devita, S. I., Mustofa, Z. N., Ainiyah, Q., & Sundoro, S. (2023). Implementasi enkrip dan dekrip file menggunakan metode Advance Encryption Standard (AES-128). *Jurnal Ilmiah Sistem Informasi dan Ilmu Komputer*.

Choiri, E. O. (2020). Implementasi kriptografi klasik pada aplikasi chat untuk menjaga kerahasiaan data. *Jurnal Teknologi dan Keamanan Informasi, 8*(2), 45–52.

Crudu, & Ana. (2025). *Build a secure login system in Vue.js with Passport.js authentication*.

Cybersecurity Ventures. (2024). *Global Cybersecurity Almanac 2024: Data Breach Statistics and Trends*. Cybersecurity Ventures Publishing.

Destriyani, D., & Painem, P. (2023). Implementasi kriptografi dengan algoritma AES-128 dan Blowfish berbasis Android pada fitur one-to-one chat Blucareer aplikasi Blucampus pada Universitas Budi Luhur. *SKANIKA: Sistem Komputer dan Teknik Informatika*.

Febitri, N., Witriyono, H., Muntahanah, M., & Marhalim, M. (2023). Application of AES 256 cryptography algorithm OCB mode on student data. *Jurnal Komputer, Informasi, dan Teknologi, 3*(2), 423–432.

Ghosh, P., Islam, M. T., Raihan, M., Farzana, F., & Ahmed Shaj, S. (2018). Apriori algorithm in rubber industry. *International Conference on Innovative Computing and Communications*, 539–550.

Han, J., Kamber, J., & Pei, J. (2021). *Data mining: Concepts and techniques*. Elsevier.

Kemp, S. (2023). *Digital 2023: Global Overview Report*. DataReportal.

Kurniawan, H., & Hidayatullah, A. (2022). Penerapan algoritma AES dan Base64 pada aplikasi pesan rahasia berbasis Android. *Jurnal Teknik Informatika (JUTIF), 3*(2), 145–152.

Mahendra, D. (2021). Secure key management strategies in mobile cryptographic applications. *International Journal of Information Security Studies*, 5(3), 145–159.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography*. CRC Press.

OECD. (2021). *The Digital Transformation: A Framework for Policy Action*. OECD Publishing.

Pereira, R., & Souza, L. (2022). A comparative analysis of password hashing algorithms for modern authentication systems. *Journal of Cybersecurity Engineering*, 6(1), 33–47.

Pradata, A., & Miraswan, K. (2020). Performance evaluation of AES and Base64 in mobile applications. *Jurnal Teknologi Informasi dan Komunikasi*, 8(2), 77–86.

Putra Utama, F., Wijaya, G., Faurina, R., & Vatresia, A. (2023). Implementasi algoritma AES 256 CBC, Base64, dan SHA-256 dalam pengamanan dan validasi data ujian online. *Jurnal Teknologi Informasi dan Ilmu Komputer*.

Ramadhani, R., & Suhartono, D. (2020). Transparansi proses enkripsi pada aplikasi mobile berbasis kriptografi modern. *Jurnal Keamanan Siber*, 4(1), 19–28.

Rohman, A. T., & Romli, M. A. (2021). Implementasi algoritma Base64 pada aplikasi kriptografi gambar untuk keamanan data visual berbasis mobile Android. *TEKNO: Jurnal Penelitian Teknologi dan Peradilan*.

Sari, M., & Mulia, N. (2020). Comparative study of bcrypt and SHA-256 for mobile authentication security. *International Journal of Mobile Computing and Security*, 3(4), 201–210.

Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C*. Wiley.

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

United Nations. (2020). *The Role of Digital Technologies and Artificial Intelligence in Achieving the Sustainable Development Goals*. United Nations Publications.

Widodo, A., & Hartati, N. (2021). Implementasi AES-128 pada aplikasi mobile untuk peningkatan keamanan data pengguna. *Jurnal Informatika dan Komputasi*, 10(1), 88–97.

Winata, A. A., Syafrullah, M., & Irawan, I. (2024). Implementasi algoritma Advanced Encryption Standard (AES-128) untuk pengamanan data berbasis web pada McDonald's Cabang T.B. Simatupang. *Jurnal TiCom: Technology of Information and Communication*.

Witriyono, H., & Fernandez, S. (2021). Implementasi enkripsi Base64, hashing SHA1 dan MD5 pada QR Code presensi kuliah. *SATIN – Sains dan Teknologi Informasi, 7*(2), 73–81.

World Economic Forum. (2023). *Future of Technology Report: Navigating the Next Wave of Digital Disruption*. World Economic Forum.