IMPLEMENTASI PENGGUNAAN BCRYPT DAN PASSKEY PADA SISTEM LOGIN WEB DI SMK NEGERI 1 XYZ

Yasir Arafat[*1], Taufik Hidayat[2], Muhammad Khozin[3]
[123] Universitas Selamat Sri, Prodi Teknik Informatika
*e-mail : [*1]yasirm000@gmail.com, [2]taufikhidayat.jc@gmail.com, [3]khozin.dsn@gmail.com*

Keamanan sistem login web merupakan aspek krusial dalam melindungi data pengguna dari berbagai ancaman siber seperti brute force, phishing, dan credential stuffing. Berbagai penelitian sebelumnya menyebutkan bahwa penggunaan algoritma hashing adaptif seperti Bcrypt mampu meningkatkan ketahanan terhadap serangan brute force karena menerapkan mekanisme salt dan cost factor yang memperlambat proses komputasi hash. Selain itu, standar autentikasi modern yang dikembangkan oleh FIDO Alliance merekomendasikan mekanisme berbasis kriptografi kunci publik (passkey) sebagai solusi autentikasi tanpa kata sandi yang lebih tahan terhadap phishing dan pencurian kredensial. Berdasarkan landasan tersebut, penelitian ini mengimplementasikan kombinasi algoritma Bcrypt dan Passkey untuk meningkatkan keamanan autentikasi pengguna pada sistem login web di SMK Negeri 1 XYZ. Metode yang digunakan adalah model Waterfall dengan tahapan analisis kebutuhan, perancangan, implementasi, pengujian, dan pemeliharaan. Pengujian sistem dilakukan menggunakan metode Black-Box Testing untuk mengevaluasi fungsionalitas dan mekanisme autentikasi. Hasil implementasi menunjukkan bahwa sistem berjalan sesuai dengan spesifikasi yang dirancang. Penerapan Bcrypt dan Passkey dalam sistem ini selaras dengan temuan pada literatur sebelumnya, yaitu berpotensi meningkatkan keamanan autentikasi serta memberikan proses login yang lebih efisien dan praktis bagi pengguna.

***Kata Kunci* — Autentikasi, Bcrypt, Enkripsi, Keamanan Siber, Passkey, Sistem Login.**

I. PENDAHULUAN

Perkembangan teknologi digital yang semakin pesat membawa dampak positif sekaligus meningkatkan risiko kejahatan siber. Tak terkecuali website yang mana pengguna dapat mengakses data ini kapan saja dan di mana saja tanpa perlu menginstal aplikasi secara lokal, sehingga menghemat ruang penyimpanan perangkat [1].Secara global, serangan terhadap sistem informasi terus mengalami peningkatan dari tahun ke tahun, khususnya pada platform berbasis web yang memanfaatkan sistem login sebagai pintu utama autentikasi. Salah satu dampak yang paling merugikan ialah kebocoran data, yang sering menjadi pemicu berbagai bentuk kejahatan siber seperti pencurian identitas dan penyalahgunaan akun digital.

Di tingkat nasional, tingginya intensitas serangan siber terlihat dari laporan Badan Siber dan Sandi Negara (BSSN), yang mencatat 448 juta serangan dalam periode Januari–Mei 2021, serta 16.233 akun sektor pemerintahan mengalami kompromi. Kepolisian juga melaporkan 3.500 kasus kejahatan siber hingga akhir Maret 2021. Jenis kejahatan yang paling banyak terjadi meliputi provokasi, penipuan online, peretasan, akses ilegal, pencurian data, hingga gangguan sistem [2]. Data ini menunjukkan bahwa keamanan autentikasi menjadi aspek yang semakin kritis bagi organisasi, termasuk lembaga pendidikan.

Seiring meningkatnya ancaman tersebut, teknologi autentikasi modern mulai dikembangkan untuk menghadirkan sistem login yang lebih aman. Salah satu inovasi terbaru adalah Passkey, teknologi autentikasi tanpa password hasil kolaborasi FIDO Alliance bersama Google, Microsoft, dan Apple. Sistem ini mengandalkan biometrik atau PIN perangkat sehingga lebih aman dari phishing dan pencurian kredensial. Studi terbaru mengenai implementasi autentikasi FIDO2 juga menegaskan bahwa teknologi Passkey mampu meningkatkan pengalaman pengguna tanpa mengorbankan aspek keamanan [3].

Selain itu, pada sistem login web tradisional, penggunaan algoritma hashing seperti Bcrypt menjadi standar keamanan untuk melindungi password. Bcrypt bekerja dengan mekanisme salt dan cost factor yang tinggi sehingga mampu menahan serangan brute force maupun rainbow table [4].

Kebutuhan akan sistem autentikasi yang kuat juga semakin relevan di lingkungan pendidikan, di mana banyak data sensitif seperti identitas siswa, guru, dan aktivitas sekolah tersimpan dalam sistem digital. SMK Negeri 1 XYZ di Kabupaten Batang. Pertambahan jumlah siswa setiap tahun membuat sistem informasi sekolah semakin kompleks, sehingga keamanan login web menjadi aspek yang krusial.

Meskipun sistem login web sekolah telah menerapkan algoritma Bcrypt, keamanan tersebut belum sepenuhnya mampu mencegah ancaman siber. Berdasarkan keterangan staf IT, Pak Yonif, pada tahun 2020 terjadi insiden peretasan yang menyebabkan server sekolah tidak

dapat diakses selama tiga hari. Investigasi menemukan adanya aplikasi cryptomining yang terinstal secara ilegal.

Algoritma hashing seperti Bcrypt juga menjadi standar dalam pengamanan data pengguna pada sistem login. Bcrypt menggunakan banyak perulangan dan salt untuk melindungi data dari serangan brute force serta rainbow table, sehingga lebih aman dibandingkan hashing konvensional [5]. Bcrypt telah diterapkan dalam berbagai framework modern, termasuk Laravel, untuk meningkatkan keamanan autentikasi pengguna. Penelitian dari Saputra dan Kurniati tahun 2026 juga menunjukkan bahwa penerapan algoritma Bcrypt dalam proses autentikasi pengguna menunjukkan peningkatan perlindungan terhadap data login melalui mekanisme penyimpanan kata sandi dalam bentuk hash, sehingga dapat meminimalkan potensi penyalahgunaan data dan meningkatkan keamanan [6]. Selain itu penelitian dari Isnaini, et al. tahun 2025 menunjukkan Implementasi Bcrypt dalam sistem web berpotensi meningkatkan keamanan autentikasi dengan memperkuat mekanisme perlindungan data pengguna, khususnya dalam menghadapi berbagai ancaman siber yang terus berkembang [7].

Melihat risiko yang ada, dibutuhkan penguatan sistem autentikasi yang lebih komprehensif. Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan kombinasi Bcrypt dan Passkey pada sistem login web SMK Negeri 1 XYZ.

II. METODE PENELITIAN

A. Alat dan Bahan Penelitian

1. Alat Penelitian
   Spesifikasi Hardware yang dibutuhkan yaitu Laptop, RAM 16 GB, dan SSD521GB. sedangkan softwere yang dibutuhkan yaitu HTML, Laravel, PHP, CSS, Passkey, Corbado, HeidiSQL, Visual Studio Code, Tailwind, Google Chrome. Ubuntu Terminal, dan Rencher Docker.
2. Bahan Penelitian
   Data pengguna yang dikumpulkan melalui kuesioner, observasi, dan wawancara. Situs web yang telah menerapkan algoritma keamanan Bcrypt. Dokumentasi teknis dan catatan sistem yang berkaitan dengan proses autentikasi. Jurnal, artikel ilmiah, dan literatur.

B. Alur Penelitian

1. Identifikasi masalah
   Melakukan proses identifikasi masalah melalui observasi dan wawancara. Langkah ini bertujuan untuk memahami kebutuhan pengguna serta berbagai kendala yang muncul dalam penggunaan sistem login.
2. Rumusan Masalah
   Mengidentifikasi pertanyaan-pertanyaan utama yang solusinya akan diperoleh melalui proses penelitian.
3. Tujuan Penelitian
   Penelitian ini bertujuan untuk merancang dan mengimplementasikan sebuah sistem login berbasis web yang aman dengan menerapkan metode enkripsi berlapis. Sistem yang dikembangkan memanfaatkan algoritma Bcrypt sebagai mekanisme pengamanan kata sandi serta teknologi Passkey sebagai metode autentikasi tambahan.
4. Studi Literatur
   Peneliti melakukan kajian terhadap berbagai sumber teori yang relevan dengan penelitian berjudul Implementasi Penggunaan Bcrpyt dan Passkey Pada Sistem Login Web.
5. Pengumpulan data
   Data dikumpulkan secara langsung dari instansi terkait dengan menerapkan prosedur yang sistematis dan terstandar melalui wawancara dan observasi.
6. Perancangan sistem
   Perancangan sistem menggunakan pendekatan berbasis objek dengan memanfaatkan Unified Modeling Language (UML). Dengan menggunakan simbol-simbol yang telah distandarkan, UML memungkinkan kita untuk membuat model sistem yang jelas, terstruktur, dan mudah dipahami [8]. Adapun model atu diagram yang digunakan dalam penelitian ini adalah use case diagram, Activity diagram, class diagram dan Sequence diagram.

C. Metode Pengembangan Sistem

Metode yang digunakan dalam pengembangan sistem penelitian ini adalah metode Waterfall. Metode waterfall adalah pendekatan pengembangan perangkat lunak yang bersifat linier, di mana setiap tahap dalam proses pengembangan harus diselesaikan terlebih dahulu sebelum melanjutkan ke tahap berikutnya [9].

1. Requirement Analysis
   Analisis kebutuhan, digunakan untuk memahami secara menyeluruh bagaimana sistem login saat ini digunakan serta masalah apa saja yang muncul dalam praktiknya.
2. System & Software Design
   Menerjemahkan kebutuan yang telah dihimpun menjadi bentuk arsitektur dan rancangan teknis yang lebih terstruktur.
3. Implementation
   Pengembangkan kode untuk sistem login berbasis web dengan mengintegrasikan Bcrypt sebagai metode hashing kata sandi dan Passkey sebagai lapisan autentikasi tambahan.
4. Unit Testing
   Tahap pengujian dilakukan untuk memastikan sistem bekerja sesuai dengan spesifikasi dengan menggunankan Black-Box Testing dan memberikan keamanan yang optimal. Tanpa mengakses struktur internal kode, pengujian ini mengevaluasi elemen-elemen antarmuka pengguna seperti menu, halaman, dan fitur untuk memastikan sistem bekerja sesuai dengan yang diharapkan [10].
5. Maintenance
   Pemantau kinerja sistem untuk memastikan keamanannya tetap terjaga. Pemeliharaan

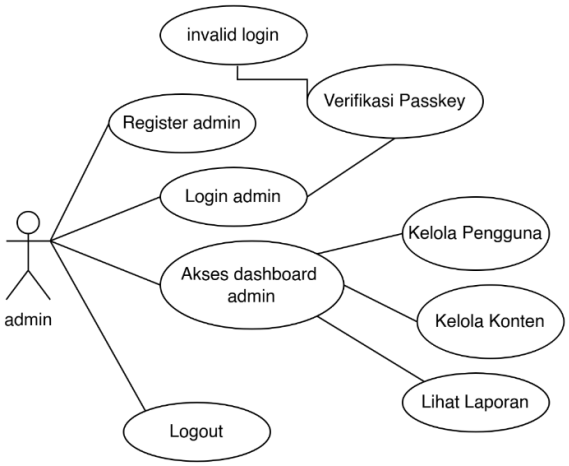
melibatkan perbaikan bug, pembaruan algoritma enkripsi jika terdapat ancaman keamanan baru, dan penyesuaian sistem sesuai dengan kebutuhan pengguna.

III. HASIL DAN PEMBAHASAN

A. Pembuatan Produk

Pada tahapan perancangan sistem, digunakan pendekatan berbasis objek dengan memanfaatkan Unified Modeling Language (UML), atau bahasa pemodelan bersatu adalah sebuah alat yang sangat berguna dalam merancang sistem yang berorientasi pada objek [8].

1. Use Case Diagram

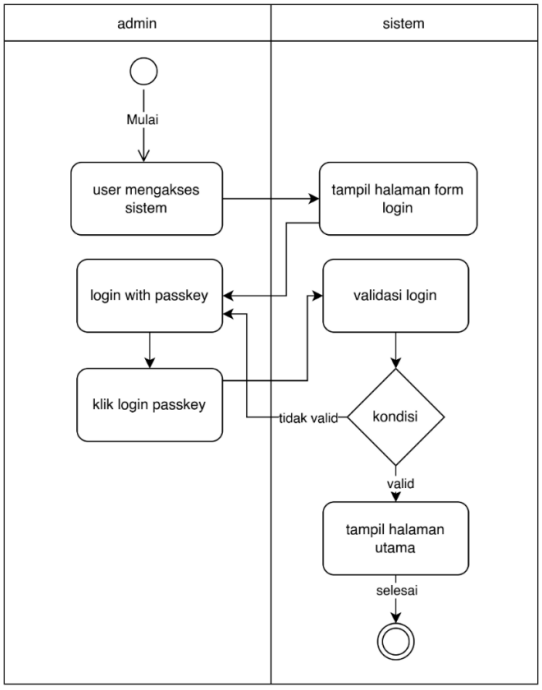


Gambar 1. Use Case Diagram

Diagram use case ini menggambarkan interaksi admin dengan sistem, dengan fokus pada keamanan login menggunakan Passkey dan fungsionalitas admin untuk mengelola sistem. Ini adalah representasi visual yang jelas dari peran admin dan kemampuan mereka dalam sistem.

2. Activity Diagram

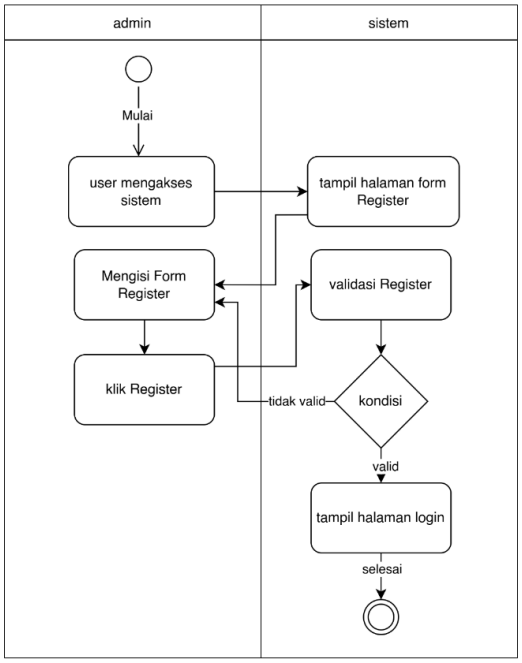
a. Activity Diagram Admin Login



Gambar 2. Activity Diagram Admin Login [11]

Diagram Activity ini menggambarkan proses login ke dalam sistem menggunakan Passkey. Admin mengakses sistem, memasukkan Passkey, dan sistem memvalidasinya. Jika valid, admin diarahkan ke halaman utama; jika tidak, admin dapat mencoba lagi. Diagram ini menekankan keamanan login dengan penggunaan Passkey dan memberikan gambaran yang jelas tentang alur login.

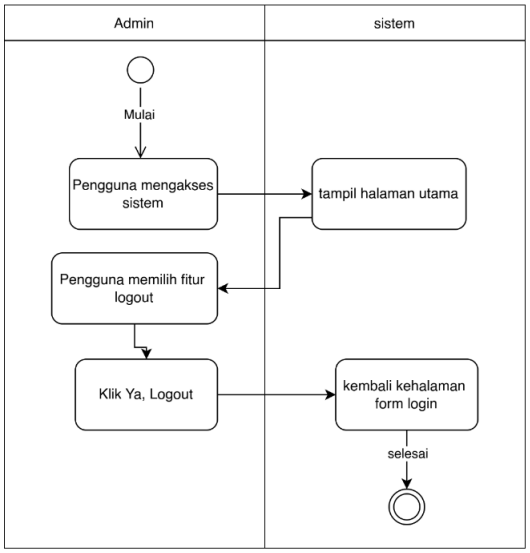
b. Activity Diagram Admin Register



Gambar 3. Activity Diagram Admin Register [12]

Activity Diagram Admin Register digunakan untuk menggambarkan alur pendaftaran pengguna, mulai dari akses sistem, pengisian formulir, validasi data, hingga berhasil login. Jika data tidak valid, pengguna diminta mengisi ulang formulir.

c. Activity Diagram Admin Logout

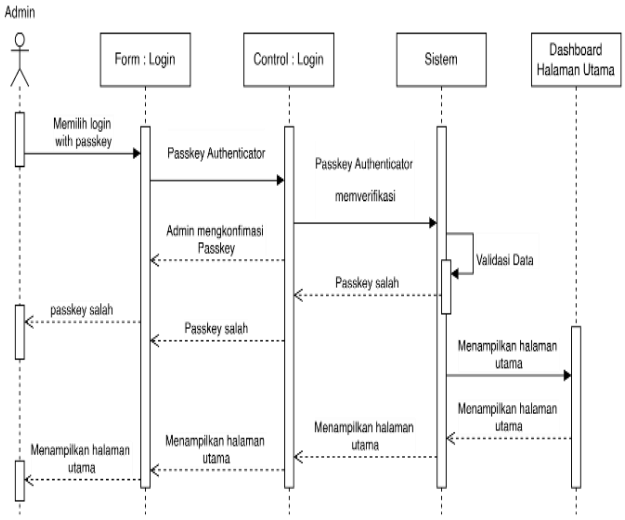


Gambar 4. Activity Diagram Admin Logout [12]

Diagram Activity ini menggambarkan proses logout admin dari sistem. Admin mengakses sistem, memilih fitur logout, mengonfirmasi pilihan mereka, dan kemudian diarahkan kembali ke halaman login.

Diagram ini memberikan gambaran yang jelas tentang alur logout.

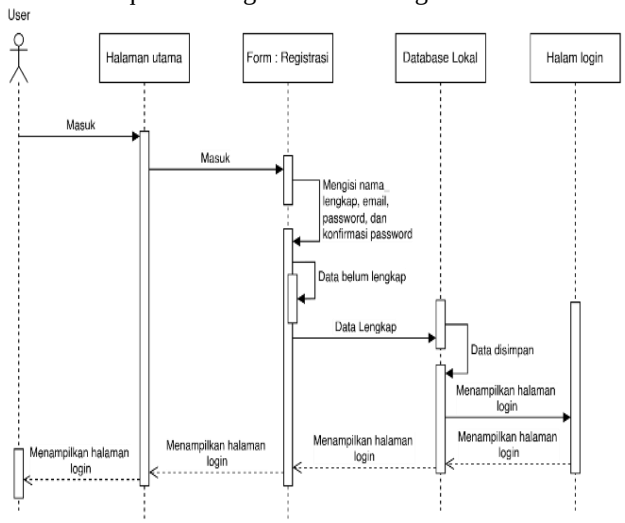
3. Sequence Diagram
   a. Sequence Diagram Admin Login



Gambar 5. Sequence Diagram Admin Login [13]

Sequence digram ini menggambarkan proses login menggunakan Passkey. Admin memilih untuk login menggunakan Passkey, sistem memverifikasi Passkey, dan jika valid, sistem menampilkan halaman utama. Jika Passkey salah, sistem menampilkan pesan kesalahan. Diagram ini memberikan gambaran yang jelas tentang interaksi antara admin dan sistem selama proses login.

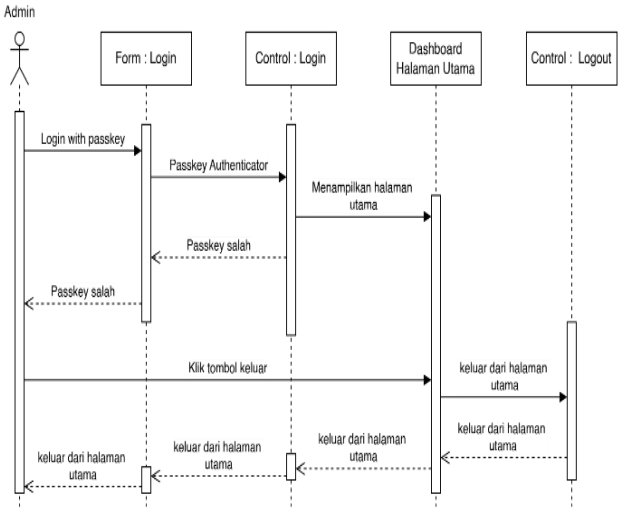
   b. Sequence Diagram Admin Register



Gambar 6. Sequence Diagram Admin Register [13]

Sequence digram ini menggambarkan alur pendaftaran pengguna. Dimulai ketika pengguna mengakses halaman utama, sistem kemudian mengarahkan pengguna ke formulir registrasi. Pengguna mengisi data pribadi seperti nama, email, dan kata sandi. Sistem memeriksa kelengkapan data. Jika data belum lengkap, pengguna diminta melengkapi. Jika data lengkap, data disimpan dalam database lokal dan sistem menampilkan halaman login kepada pengguna.

   c. Sequence Diagram Admin Logout



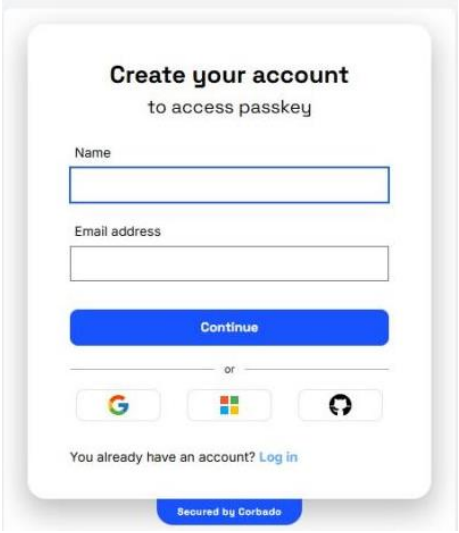
Gambar 7. Sequence Diagram Admin Logout [13]

Sequence digram ini menggambarkan proses login dan logout menggunakan Passkey. Admin memilih untuk login menggunakan Passkey, sistem memverifikasi Passkey, dan jika valid, sistem menampilkan halaman utama. Admin kemudian dapat mengklik tombol keluar untuk logout. Jika Passkey salah, sistem menampilkan pesan kesalahan. Diagram ini memberikan gambaran yang jelas tentang interaksi antara admin dan sistem selama proses login dan logout.

4. Tampilan antar muka sistem
   a. Tampilan HomePage

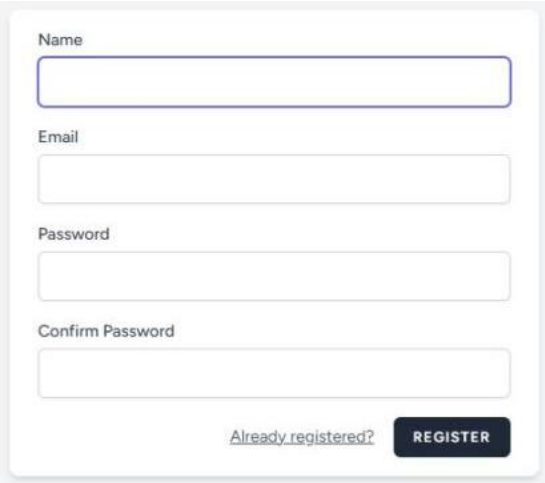
Gambar 8. Tampilan Halaman Home

   b. Tampilan Form Login



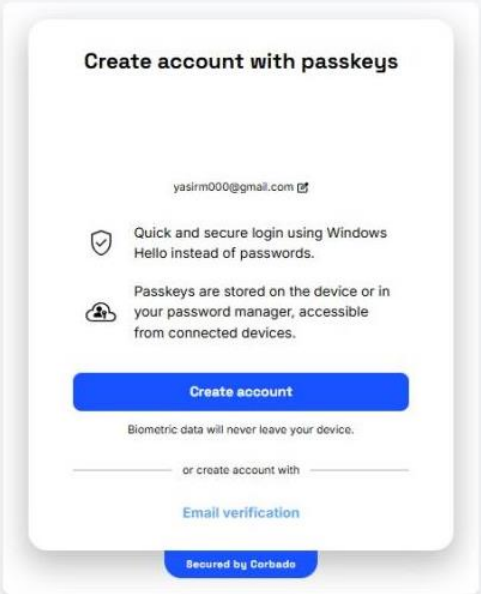
Gambar 9. Tampilan From Login

c. Tampilan Form Register



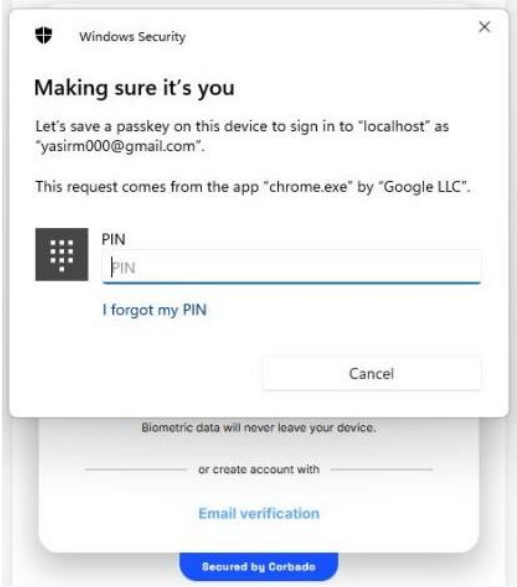
Gambar 10. Tampilan Form Register

d. Tampilan Form Create Passkey



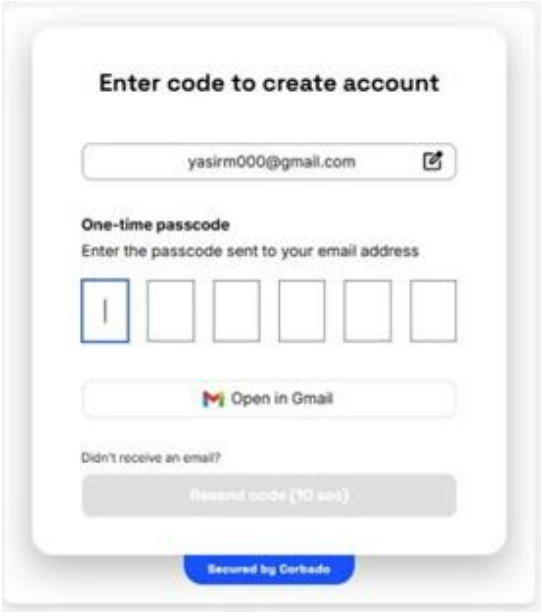
Gambar 11. Tampilan Form Create Passkey

e. Tampilan Form Create Private Key



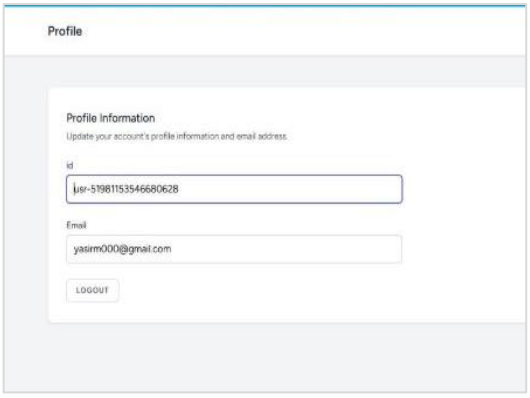
Gambar 12. Tampilan Form Cretae Private Key

f. Tampilan Verifikasi Pembuatan Passkey



Gambar 13. Tampilan Verifikasi Pembuatan Passkey

g. Tampilan Dashbord Admin



Gambar 14. Dashboard Admin

5. Pengujian Produk

Pengujian Black-Box Testing merupakan metode verifikasi yang digunakan untuk mengevaluasi antarmuka pengguna dalam sebuah sistem. Prosedur ini dilakukan untuk memastikan bahwa setiap fitur dapat berfungsi dengan baik, mulai dari kemampuan sistem menerima input dengan benar, menghasilkan output yang akurat, hingga memastikan integrasi dengan sumber data eksternal seperti arsip maupun basis databerjalan tanpa kendala. Bentuk penerapan Black-Box Testing dalam penelitian ini ditampilkan pada tabel-tabel berikut.

Tabel 1. Pengujian Sistem Login

Pengujian 1: Pengujian pada *form login*				
No	Deskripsi pengujian	Hasil yang diharapkan	Hasil pengujian	Kesimpulan

Pengujian 1: Pengujian pada *form login*				
1	Mengklik emal yang telah didaftar "yasir 000@gmail.com", dengan *Passkey*	Data berhasil masuk ke dalam *database* dan pengguna ke halaman "*Form* Masuk"	Sesuai harapan	Sesuai
2	Memasukkan, *email* "exmoomaster@gmail.com", dengan *Passkey*	Muncul pesan bahwa *email* belum terdaftar *Passkey*	Sesuai harapan	Sesuai

Pengujian 2: Pengujian Menggunakan Perangkat Berbeda				
No	Deskripsi pengujian	Hasil yang diharapkan	Hasil pengujian	Kesimpulan
1	Memastikan bahwa public key hanya tersimpan pada server WebAuth	Data berhasil tersimpan 1 user public key pada WebAuth corbado	Sesuai harapan	Sesuai
2	Memasukkan, *email* "yasirm000@gmail.com", dengan metode lain	Terdapat pilihan keamanan lain, yaitu pin, dan email	Sesuai harapan	Sesuai
3	Menggunakan perangkat yang berbeda dengan akun yang terdaftar	Data *Passkey* belum terdaftar, verifikasi ulang dengan 2FA melalui email	Sesuai harapan	Sesuai

Pengujian 3: Pengujian pada Tampilan *Database*				
No	Deskripsi pengujian	Hasil yang diharapkan	Hasil pengujian	Kesimpulan
1	Tampilan *Database*	Menu "*Password*" sudah terenkripsi *Bcrypt*	Sesuai harapan	Sesuai

6. Hasil Akhir

Gambar 15. Gambaran Umum Hasil Produk

Berdasarkan hasil pengujian Balck-box testing dari website tersebut dihasilkan tidak ditemukan kesalahan fungsionalitas pada tahap pengujian dari yang di inputkan dengan apa yang diharapkan semuanya sesuai.

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan proses implementasi disimpulkan bahwa penerapan algoritma Bcrypt berkontribusi dalam meningkatkan keamanan penyimpanan kata sandi. Hal ini sejalan dengan berbagai penelitian sebelumnya yang menyatakan bahwa Bcrypt dirancang dengan mekanisme adaptive hashing yang memperlambat proses komputasi sehingga lebih tahan terhadap serangan brute force dibandingkan metode hashing konvensional.

Selain itu, penerapan teknologi Passkey juga menunjukkan peningkatan dari sisi keamanan dan efisiensi autentikasi. Sejumlah literatur dan standar autentikasi modern menyebutkan bahwa mekanisme berbasis kriptografi kunci publik seperti dalam standar FIDO mampu mengurangi risiko phishing, pencurian kredensial, dan serangan berbasis database karena tidak menyimpan kata sandi dalam bentuk yang dapat digunakan ulang. Dengan demikian, hasil implementasi dalam penelitian ini selaras dengan temuan pada penelitian terdahulu, yaitu bahwa kombinasi Bcrypt dan mekanisme autentikasi berbasis Passkey dapat meningkatkan kualitas sistem login dari aspek keamanan.

B. Saran

Penelitian selanjutnya dapat menguji dari segi keamanan secara menyeluruh baik dari Session, Cache, Man In Midle, Brute force dll, mengembangkan fitur tambahan seperti Multi-Factor Authentication (MFA), pemulihan akun yang lebih aman, dan notifikasi aktivitas login mencurigakan.

Evaluasi keamanan dapat diperdalam melalui pengujian penetrasi, analisis kerentanan berkala, dan evaluasi efektivitas sistem terhadap serangan siber. Peningkatan usabilitas dapat difokuskan pada desain antarmuka yang intuitif, proses registrasi/login yang lebih cepat, dan panduan pengguna yang komprehensif. Integrasi sistem login dengan sistem lain di SMK Negeri 1 XYZ, seperti sistem akademik atau perpustakaan, juga disarankan.

DAFTAR PUSTAKA

[1] Asa Dilla Safitri, Atik Sulami, Jamilatun Safitri, and Dwi Hartanti, "Perancangan aplikasi belajar bahasa Inggris berbasis website," TEKNOSAINS J. Sains, Teknol. dan Inform., vol. 10, no. 1, pp. 12–19, Jan. 2023, doi: 10.37373/tekno.v10i1.251.

[2] Naylawati Bahtiar, "Darurat Kebocoran Data : Kebutuhan Regulasi Pemerintah," Dev. Policy Manag. Rev., vol. 2, no. 1, pp. 1–16, 2022.

[3] M. Kepkowski, M. Machulak, I. Wood, and D. Kaafar, "Challenges with Passwordless FIDO2 in an Enterprise Setting: A Usability Study," Proc. - 2023 IEEE Secur. Dev. Conf., pp. 37–48, 2023, doi: 10.1109/SecDev56634.2023.00017.

[4] Developer Google, "Passwordless login with passkeys | Authentication." 2023.

[5] G. D. M. Zulma, H. B. Seta, and T. Yuniati, "Implementasi Algoritma Aes Dan Bcrypt Untuk Pengamanan File Dokumen," Inform. J. Ilmu Komput., vol. 18, no. 2, p. 163, 2022, doi: 10.52958/iftk.v18i2.4667.

[6] A. Saputra et al., "Aplikasi Penjualan Udang Pepai Berbasis Web Dengan," JATI (Jurnal Mhs. Tek. Inform., vol. 10, no. 1, pp. 726–733, 2026.

[7] K. Nur, D. Suhartono, M. Thoriq, and A. Qothrunnada, "Implementasi Pengamanan Data Menggunakan Teknik Bcrypt Hashing Password dan Algoritma Advanced Encryption Standard (AES) Implementation of Data Security Using Bcrypt Hashing Password Technique and Advanced Encryption Standard (AES) Algorithm," J. Sist. dan Teknol. Inf., vol. 13, no. 1, pp. 101–108, 2025, doi: 10.26418/justin.v13i1.84997.

[8] A. Indriati, "Penerapan algoritma aes pada keamanan url studi kasus website mahasiswa atma luhur," Institut Sains dan Bisnis Atma Luhur, 2023.

[9] H. Aspriyono, "Implementasi Metode Waterfall Dalam Pembuatan E-Learning Pada SMK Teknik PAL Surabaya Menggunakan Codeigniter Dan MySQL," SIMKOM, vol. 6, no. 1, pp. 58–65, Jan. 2021, doi: 10.51717/simkom.v6i1.55.

[10] A. A. Arbeit, D. Ramadhanti, R. Alief, R. Akbar, S. Ramadhan, and A. Saifudin, "Black box testing on best sales selection system application using equivalence partitions techniques," Bisnis Dan Pendidik., vol. 1, no. 1, pp. 101–106, 2023.

[11] Y. Y. Carlos, R. Rino, and E. Edy, "Implementasi sistem monitoring jaringan berbasis web menggunakan Mikrotik," J. Algor, vol. 5, no. 2, pp. 1–10, 2024.

[12] B. S. A. Pradana and I. G. A. S. Sidhimantra, "Pembuatan sistem informasi perencanaan stok barang berbasis website menggunakan metode Material Requirement Planning (MRP): Studi kasus Toko Jaya Sembako," Universitas Negeri Surabaya, 2024.

[13] D. C. Darmadi, N. I. Utama, and F. M. Al Anshary, "Perancangan frontend website pengelolaan data pemilu berbasis blockchain untuk pemilihan presiden & wakil presiden dengan metode design thinking (Studi kasus: KPU Kota Bandung)," Universitas Telkom, 2024.