Rental Mobil Berbasis Web Menggunakan Sistem Keamanan Hashing Blowfish dan Watermarking

Rehan Angger P.[1], **Ramadhan Renaldy**[2] **dan Dzulfiqar Alang S.**[3]

Jurusan Informatika, Fakultas Teknik dan Informatika, Universitas PGRI Semarang

Gedung B Lantai 3, Kampus 1 Jl. Sidodadi Timur 24, Semarang

E-mail : anggerrehan6@gmail.com[1], ramadhanrenaldy@upgris.ac.id[2], dzulfiqaralang1@gmail.com[3]

Abstrak

Permasalahan utama dalam sistem rental mobil berbasis web adalah risiko keamanan data pelanggan, seperti pencurian data pribadi dan penipuan identitas. Selain itu, sistem tradisional sering kali tidak efisien dan kurang fleksibel dalam pengelolaan layanan. Oleh karena itu, proyek ini bertujuan untuk mengembangkan sistem rental mobil berbasis web yang tidak hanya efisien, tetapi juga mengutamakan keamanan data pelanggan. Dalam sistem ini, digunakan teknologi hashing Blowfish untuk mengamankan kata sandi pengguna. Blowfish dipilih karena kemampuannya untuk memperlambat serangan brute force melalui penerapan mekanisme salt dan iterasi biaya. Selain itu, dokumen keuangan seperti faktur dilindungi menggunakan watermark untuk mencegah manipulasi data atau distribusi yang tidak sah. Hasil implementasi menunjukkan bahwa sistem ini memberikan pengalaman pengguna yang mudah, mulai dari pendaftaran hingga penyewaan mobil, dengan fitur keamanan yang kuat. Pengguna dapat mencetak invoice dengan watermark, sementara administrator dapat mengelola data mobil, pelanggan, transaksi, dan laporan melalui antarmuka yang sederhana namun fungsional. Dengan demikian, sistem ini mampu meningkatkan efisiensi sekaligus memberikan tingkat keamanan yang optimal bagi pelanggan dan penyedia layanan.

***Kata Kunci*:** Sistem rental mobil berbasis web, Hashing Blowfish, Watermark

I. PENDAHULUAN

Di era digital saat ini, penggunaan internet dan teknologi informasi telah membawa perubahan besar dalam berbagai sektor, termasuk dalam dunia bisnis. Salah satu sektor yang mengalami perkembangan signifikan adalah bisnis rental mobil. Semakin banyak masyarakat yang mengandalkan layanan rental mobil untuk memenuhi kebutuhan transportasi mereka, baik untuk perjalanan wisata, bisnis, maupun kebutuhan pribadi. Namun, dengan meningkatnya permintaan, tantangan dalam pengelolaan layanan ini pun semakin kompleks.

Sistem bisnis konvensional yang mengandalkan komunikasi langsung atau telepon sering kali dianggap kurang efisien dan tidak fleksibel. Pelanggan harus datang langsung ke kantor penyedia layanan atau melakukan reservasi secara manual, yang memakan waktu dan usaha lebih. Seiring dengan perkembangan teknologi, banyak bisnis mulai beralih ke platform digital melalui sistem e-commerce. Bisnis rental mobil tidak terkecuali; saat ini, banyak perusahaan yang berusaha memanfaatkan teknologi ini untuk menawarkan layanan yang lebih efisien, cepat, dan mudah diakses oleh pelanggan.

Meskipun bisnis rental mobil telah beralih ke e-commerce, masih terdapat beberapa tantangan yang signifikan dalam pengoperasiannya. Salah satu tantangan terbesar adalah keamanan data pelanggan. Pada platform e-commerce, informasi sensitif seperti identitas pelanggan, detail transaksi, serta data pribadi lainnya menjadi sangat rentan terhadap pencurian atau penyalahgunaan. Keamanan ini menjadi isu utama dalam pengembangan sistem rental mobil berbasis internet, karena kepercayaan pelanggan terhadap keamanan sistem sangat mempengaruhi reputasi bisnis tersebut. Selain itu, verifikasi identitas pengguna secara online sering kali menimbulkan risiko penipuan, seperti penggunaan identitas palsu atau pencurian

data. Oleh karena itu, diperlukan sistem keamanan yang kuat untuk melindungi data pelanggan dan menjaga integritas transaksi yang terjadi.

Saat ini, umumnya fungsi hash, seperti MD5 atau SHA256, memiliki kemampuan untuk melakukan digest pesan dengan sangat cepat karena sering digunakan sebagai tanda tangan digital pada pesan dengan ukuran yang besar. Untuk ukuran pesan yang besar, digest pesan yang cepat bukanlah masalah.Namun, hal ini berbeda untuk kata sandi, dimana Panjang kata sandi umumnya singkat dan terbatas, serta jumlah maksimal kombinasi yang dapat dilakukan pada kata sandi bisa diperkirakan. Dengan begitu, kecepatan digest pesan dari fungsi hash justru menjadi kelemahan tersendiri, yaitu jika penyerang menggunakan brute force untuk melakukan autentikasi, maka dalam waktu singkat autentikasi dapat ditembus berkat kecepatan fungsi hash dalam men-digest kata sandi.

Maka dari itu, digunakan fungsi hash khusus yang diperuntukan untuk men-digest kata sandi, dimana fungsi hash ini memakan waktu untuk melakukan digest kata sandi dan perkembangan perangkat keras tidak akan cukup membantu untuk mempercepat proses digest kata sandi. Fungsi hash ini disebut juga dengan password hash. Salah satu jenis dari password hash adalah BCrypt.

II. METODOLOGI PENELITIAN

2.1. Rental Mobil

Rental mobil merupakan usaha yang menawarkan jasa penyewaan mobil kepada pihak yang membutuhkan, baik perorangan maupun perusahaan. Penyewa tidak bertanggung jawab terhadap maintenance mobil, namun pemilik rental mobil sangat penting menjaga kondisi mobil karena kunci sukses rental mobil adalah menjaga biaya biaya perawatan mobil untuk selalu lebih rendah. Selain dianggap lebih praktis, untuk mendapatkan mobil sewaan ini memang tergolong mudah, asalkan konsumen dapat memenuhi beberapa persyaratan yang ditentukan perusahaan atau pihak penyewa mobil. Keuntungan lain, masyarakat tidak perlu repot-repot untuk membeli mobil. Komponen-komponen yang dipersiapkan untuk membuka usaha rental mobil adalah:

- Prasarana dan sarana, seperti:
    a. Tempat atau lokasi yang strategis
    b. Tenaga ahli yang cukup berpengalaman di bisnis rental mobil
    c. Modal usaha yang cukup
    d. Perijinan
- Perencanaan dan Pengendalian Keuangan
    a. Proyeksi arus kas (jangan lupa masukkan biaya cadangan penyusutan kendaraan)
    b. Melakukan administrasi dan pembukuan yang teratur, seperti catatan data-data pelanggan, catatan barang inventaris kantor, catatan keluar masuknya uang/hari (buku kas harian) dan lain-lain
    c. Catatan laba rugi/ bulanan
- Perencanaan Strategi Pemasaran
    a. Penetapan harga sewa mobil dan cara pembayaran
    b. Penentuan target market, masyarakat dari kelas ekonomi apakah yang menjadi sasaran anda
    c. Variasi jasa yang ditawarkan untuk member nilai lebih pada rental mobil anda
    d. Promosi untuk menarik perhatian konsumen.

E-ISSN: 2985-3532

- Administrasi yang bagus dan legalitas dari kontrak perjanjian sewa kendaraan
- Atasi kerugian kendaraan dengan asuransi mobil

2.2. Fungsi Hash

Fungsi hash merupakan salah satu jenis dari kriptografi dimana suatu pesan dilakukan enkripsi dalam ukuran tertentu. Keunikan dari fungsi hash adalah suatu pesan yang telah dienkripsi dengan fungsi hash tidak mungkin dilakukan dekripsi agar dapat dikembalikan isi dari pesan tersebut. Selain itu, ukuran dari pesan yang dihasilkan oleh fungsi hash akan selalu sama, berapapun ukuran pesan yang dimasukkan.Keunikan dari fungsi hash ini dapat digunakan untuk melakukan autentikasi dan verifikasi suatu informasi yang diterima dengan informasi yang telah tersimpan sebelumnya.Pencocokkan dilakukan dalam bentuk hasil dari fungsi hash.

Fungsi hash sendiri memiliki beberapa sifat tertentu yang mendefinisikan bahwa fungsi hash tersebut bekerja dengan baik yaitu: - Collision Resistance: sifat ini diartikan bahwa akan sulit bagi fungsi hash untuk menghasilkan sebuah nilai yang sama dari dua buah pesan yang berbeda. Sebagai contoh, jika terdapat suatu fungsi hash H(x) dan dua buah pesanadanbdimana $a \neq b$, maka sangat kecil kemungkinan untuk mendapatkan H(a)=H(b). - Preimage Resistance: sifat ini diartikan bahwa jika terdapat sebuah hasil fungsi hash, akan sangat sulit mencari pesan yang memiliki hasil fungsi hash yang sama. Sebagai contoh, semisal telah terdapat hasil fungsi hash H(x) berupa y, akan sulit untuk menemukan sembarang pesan a dimana H(a) =y. - Second Preimage Resistance: sifat ini diartikan bahwa jika terdapat pasangan pesan dan hasil fungsi hash, akan sulit untuk menemukan hasil fungsi hash yang sama dengan pasangan pesan dan hasil fungsi hash yang telah diketahui dari pesan yang berbeda. Sebagai contoh, jika terdapat pasangan pesanan dan hasil fungsi hash H(x) berupa H(a) = y, makaakansulituntuk mencari pesan b dimana hasil dari fungsi hashpadapesan b H(b) = y = H(a). Dengan sifat-sifat tersebut, maka tingkat keamanan di suatu fungsi hash dapat diketahui berdasarkan apakah sifat tersebut sudah berhasil dipecahkan atau belum.

2.3. Blowfish Cipher

Blowfish cipher merupakan salah satu jenis dari algoritma cipher blok yang dikembangkan oleh Bruce Schneier pada tahun 1993 sebagai alternatif algoritma cipher blok DES. Blowfish cipher menggunakan blok dengan ukuran 64-bit, kunci dengan ukuran bervariasi antara 32-bit hingga 448-bit, subkunci sebanyak 18 buah, putaran sebanyak 16 kali, dan 4 buah substitution box (S-Box). Untuk tahap pembuatan subkunci, pada awalnya terdapat 18 buah subkey yang nilainya telah diinisialisasi dan disimpan pada sebuah array sebagai berikut.

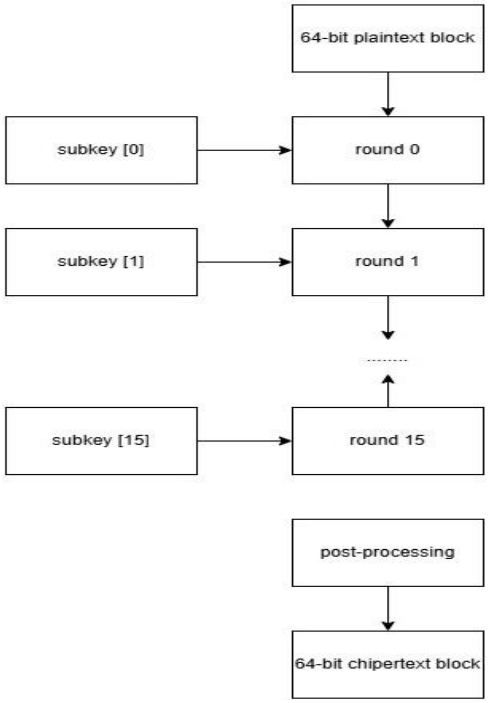
E-ISSN: 2985-3532

Subkey[0] :243f6a88 Subkey[9] :38d01377
Subkey[1] :85a308d3 Subkey[10]:be5466cf
Subkey[2] :13198a2e Subkey[11]:34e90c6c
Subkey[3] :03707344 Subkey[12]:c0ac29b7
Subkey[4] :a4093822 Subkey[13]:c97c50dd
Subkey[5] :299f31d0 Subkey[14]:3f84d5b5
Subkey[6] :082efa98 Subkey[15]:b5470917
Subkey[7] :ec4e6c89 Subkey[16]:9216d5d9
Subkey[8] :452821e6 Subkey[17]:8979fb1b

Gambar 30. Skema Enkripsi Pada Blowfish Cipher

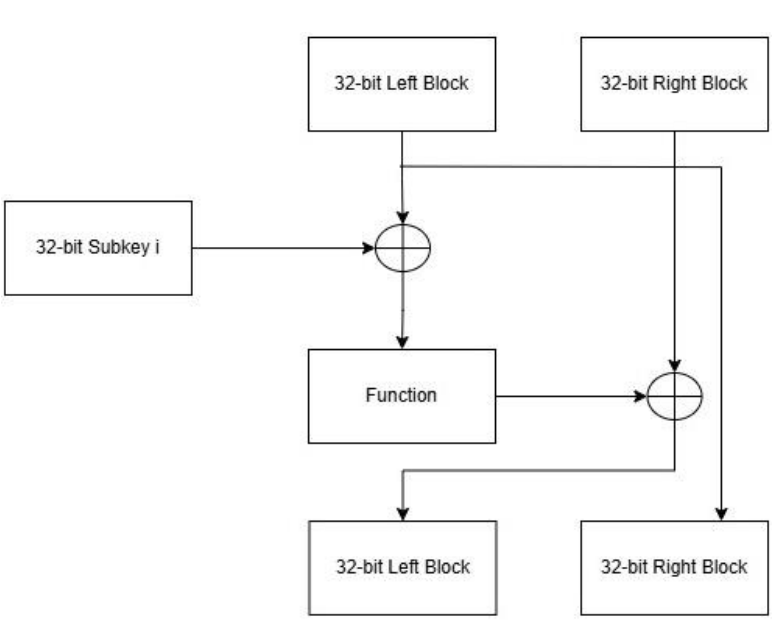
Lalu, setiap subkunci tersebut dilakukan operasi XOR dengan kunci dari input yang dibagi per 32-bit secara sekuensial. Sebagai contoh, subkunci pertama di XOR dengan blok kunci pertama, subkunci kedua di XOR dengan blok kunci kedua, dan seterusnya. Jika jumlah blok kunci kurang dari 18, maka setelah melakukan XOR pada blok kunci terakhir, untuk subkunci berikutnya dilakukan XOR dengan blok kunci pertama. Sebagai contoh, jika kunci sepanjang 64- bit, maka akan didapat dua buah blok kunci. Untuk proses pembentukan kunci, pada subkunci pertama di XOR dengan blok kunci pertama, lalu pada subkunci kedua di XOR dengan blok kunci kedua. Untuk subkunci ketiga, karena jumlah blok kunci hanya dua, maka urutan blok kunci yang dipilih dimulai dari awal lagi, sehingga subkey ketiga di XORdenganblokkunci pertama. Setelah semua subkunci telah diproses, barulah masuk ke dalam proses enkripsi Blowfish cipher.

Secara keseluruhan, alur dari enkripsi pada blowfish cipher adalah sebagai berikut.



Gambar 2. Skema Enkripsi Pada Blowfish Cipher

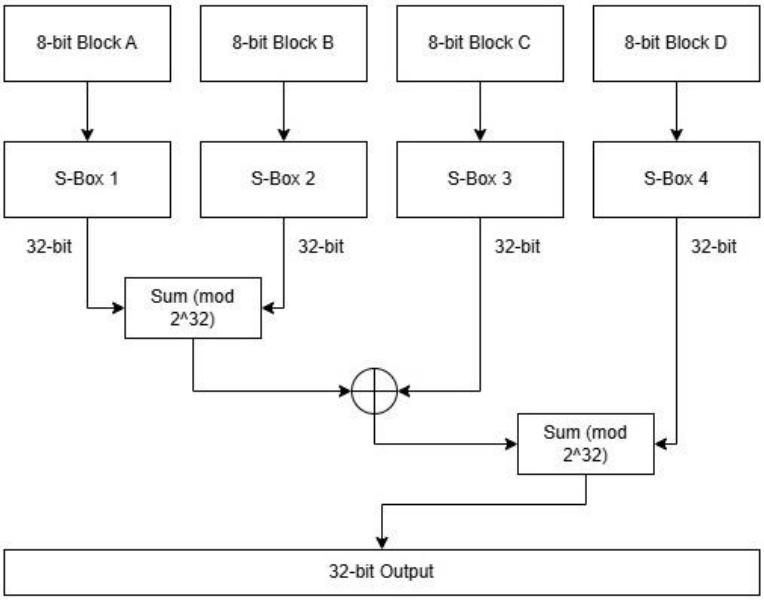
Pada setiap rondenya, enkripsi dilakukan dengan menggunakan jaringan feistel sebagai berikut.



Gambar 3. Jaringan Feistel Pada Blowfish Cipher

Pertama-tama blok pesan 64-bit dibagi menjadi 32-bit blok kiri dan 32-bit blok kanan. Lalu, pada blok kiri dilakukan operasi XOR dengan subkunci untuk putaran ke-i. setelah itu,hasil XOR dimasukkan ke dalam fungsi. Hasil dari fungsi tersebut lalu di XOR dengan blok kanan dan disimpan sebagai blok kiri yang baru. Sementara untuk blok kanan yangbaru menggunakan nilai blok kiri sebelum dilakukan operasi. Fungsi yang dijelaskan pada jaringan feistel dijelaskan sebagai berikut.

E-ISSN: 2985-3532



Gambar 4. Fungsi pada Jaringan Feistel

Di dalam fungsi, input blok dengan ukuran 32-bit dibagi secara sekuensial menjadi 4 buah blok yang masing-masing berukuran 8-bit. Lalu, dari dilakukan proses substitusi pada tiap blok dengan S-Box yang telah didefinisikan sebelumnya. Blok 8-bit pertama disubstitusi dengan S-Box pertama, blok 8- bit kedua dengan S-Box kedua, dan seterusnya. Lalu, hasil dari substitusi pada blok pertama dan kedua dijumlahkan dan di modulo dengan 2 32 . Hasil dari penjumlahan tersebut kemudian di XOR dengan hasil substitusi pada blok ketiga, lalu diteruskan dengan menjumlahkan hasil dengan hasil substitusi blok keempat dan di modulo 2 32 . Hasil ini kemudian dijadikan output dari fungsi tersebut. Setelah melalui seluruh ronde, terdapat post-processing pada cipherteks sebelum dikembalikan sebagai output.

2.4. BCrypt

BCrypt merupakan sebuah fungsi hash yang dibuat oleh Niels Provos dan David Mazières dengan berdasarkan Blowfish cipher. Penamaan BCrypt terdiri dari B untuk Blowfish dan Crypt yang merupakan nama fungsi hash yang digunakan pada sistem kata sandi di UNIX. Crypt pada awal pengembangannya di tahun 1976 hanya dapat melakukan hash maksima untuk empat buah kata sandi setiap detiknya, hal ini yang membuat fungsi hash Crypt cukup kuat pada waktunya. Namun, seiring dengan pesatnya perkembangan teknologi, sebuah komputer saat ini dengan software dan hardware yang telah dioptimalisasi dapat melakukan hashing dengan Crypt sebanyak 200.000kata sandi per detik. Maka dari itu, fungsi hash Crypt sendiri saat ini sudah tidak cocok jika digunakan untuk menjaga keamanan kata sandi. Pada BCrypt, fungsi hash Crypt dikombinasikan dengan Blowfish cipher agar waktu yang dibutuhkan untuk melakukan hashing menjadi lebih lama. Blowfish cipher sendiri sebenarnya merupakan block cipher yang cukup cepat, kecuali saat melakukan pergantian kunci.

Pada Blowfish Cipher, setiap kali pembuatan kunci yang baru membutuhkan waktu pemrosesan awal yang setara dengan waktu yang dibutuhkan untuk melakukan enkripsi pada teks berukuran empat kilobytes.Lamanya waktu proses yang dibutuhkan untuk membuat kunci baru pada Blowfish cipher inilah yang dimanfaatkan sebagai kebutuhan komputasi tambahan dalam BCrypt. Sehingga,serangan brute force pada kata sandi yang menggunakan fungsi hash BCrypt dapat diperlambat. Pada prosesnya, BCrypt memiliki tahap inisialisasi kunci yang dikembangkan dari tahap inisialisasi kunci pada Blowfish cipher, yang diberi nama “eksblowfish”, kepanjangan dari“expensive key schedule Blowfish”. Selain itu, BCrypt

E-ISSN: 2985-3532

juga secara default menggunakan 128-bit salt pada proses hashingnya untuk mencegah serangan rainbow table. Proses BCrypt sendiri terbagi menjadi dua tahap. Tahap Pertama Adalah menjalankan inisialisasi kunci eks blowfish dengan parameter berupa cost yang diinginkan, nilai salt, dan kata sandi yang akan di hashing. Pada tahap ini, BCrypt akan melakukan melakukan penurunan kunci, dimana sekumpulan subkunci diturunkan dari sebuah kunci utama, dengan kunci utama diisi oleh kata sandi. Jika kata sandi yang digunakan terlalu pendek, pada tahap ini nantinya akan dibuat menjadi kunci yang lebih panjang. Sehingga, tahap pertama juga dapat dikatakan melakukan penguatan pada kunci. Lalu, pada tahap kedua dilakukan enkripsi pada sebuah magic value dengan ukuran 192-bit "Orphan BeholderS cry Doubt" menggunakan kunci yang telah dibuat pada tahap pertama dan dilakukan titrasi sebanyak 64 kali. Hasil akhir dari tahap ini adalah hasil enkripsi menggunakan mode ECB yang digabungkan dengan cost serta nilai salt yang berukuran 128-bit.

2.5. Tinjauan Literatur

Pada bagian tinjauan literatur kami mendapatkan 2 jurnal sebagai inspirasi dari sistem yang kami buat. Berikut rangkuman ke-lima jurnal yang kami dapatkan.

Judul Jurnal	Penulis	Tahun Terbit	Metode	Hasil	Kesimpulan
Analisis Penggunaan Fungsi Hash BCrypt untuk Keamanan Kata Sandi(Naufal Yafie, 2020)	Hilmi Naufal Yafie	2020	Dienkripsi dengan fungsi hash Hash Crypt dikombinasikandengannBlowfish cipher Eksperimen terhadap 20 fungsi hash	BCrypt 265 [$2a$05$.OSesZjz0y92ZQKbWpivHuEUQGSBuJ.03oE3RnCjKm.IsqBeBf.™] (SHA-256) dengan nilai 12030 hash per detik, NTLM Hash dengan nilai 29312 hash per detik, MS DCC dengan nilai 33057 hash per detik, Cisco PIX dengan nilai 14347 hash per detik, Cisco Type 7 dengan nilai 23571 hash per detik, MS SQL 2020 dengan nilai 15598 hash per detik, MySQL dengan nilai 28628 hash per detik, Postgres (MD5) dengan nilai 25859 hash per detik, LDAP (MD5) dengan nilai 15260 hash per detik, dan LDAP (SHA-1) dengan nilai 49912 hash per detik. Bahkan, terdapat beberapa fungsi hash yang memiliki nilai diatas 100000, yaitu SHA-1 dengan nilai 465116 hash per detik, SHA-256 dengan nilai 418410 hash per detik, SHA-512 dengan nilai 223214 hash per detik, dan MD5 dengan nilai 478468 hash per detik.	Dari hasil eksperimen yang telah dilakukan, didapatkan bahwa BCrypt mendapatkan nilai hash per detik terkecil diantara 20 fungsi hash yang diuji, yaitu 265 hash per detik. Maka dari itu, dapat dikatakan bahwa BCrypt memiliki keamanan terbaik diantara 20 fungsi hash yang duji dalam mencegah penyerangan brute force pada kata sandi yang di hashing. Selain BCrypt, terdapat pula beberapa fungsi hash lain yang dapat digunakan sebagai fungsi hash alternatif untuk menjaga keamanan kata sandi dari penyerangan brute force, seperti DES, Oracle 10, dan APR1.

WATERMARK DENGAN GABUNGAN STEGANOGRAFI DAN VISIBLE WATERMARKING (Rosmiyati & Mulyana, 2018)	Juni Rosmiyati, Teady Matius Surya Mulyana,	2018	Visible Watermarking Merupakan jenis watermark dapat dilihat oleh panca indra manusia (mata telanjang).	Pada tahap ini dilakukan implementasi (pengkodean) berdasarkan rancangan yang dilakukan pada tahap sebelumnya. Dibangun suatu aplikasi watermarking menggunakan metode Invisible Watermarking pada domain DWT. Modul yang dibangun meliputi proses penyisipan dan ekstraksi. Bahasa pemrograman yang digunakan pada tahap implementasi ini yaitu bahasa pemrograman Matlab R2013a.	Aplikasi watermarking yang telah dibuat memiliki tingkat invisibility yang bagus, artinya watermark yang disisipkan tidak terlihat, hal ini dapat dibuktikan dengan nilai PSNR yang cukup tinggi.
Blowfish Advanced CSUntuk Solusi Keamanan Sistem Komputer Sekolah (Syafar et al., 2023)	Faisal Syafar, Halimah Husain, Sutarsih Suhaeb, Putri Ida, Supriadi	2023	Penelitian ini menggunakan metode kualitatif dengan studi kasus untuk mengimplementasikan algoritma Blowfish Advanced CS dalam pengamanan data digital. Proses enkripsi dan dekripsi	Hasil menunjukkan algoritma ini efektif menjaga kerahasiaan data, di mana data yang dienkripsi hanya dapat diakses dengan kunci yang sesuai. Proses ini memastikan integritas dan keamanan informasi, menjadikannya cocok untuk aplikasi di lingkungan pendidikan.	algoritma Blowfish Advanced CS adalah metode yang efisien dan aman untuk melindungi data digital. Dengan proses key setup yang memperkuat algoritma, sistem ini mampu menjaga integritas dan kerahasiaan data.

			menggunakan kunci simetris minimal empat karakter dengan kombinasi kunci dan S-box pada key setup untuk memperkuat algoritma.		
Pengamanan File Audio Menggunakan Algoritma Kriptografi Blowfish Dan Pengujian UAT(Amsari et al., 2021)	Siswanto, Farizal Dias Amsari, Basuki Hari Prasetyo, Wahyu Pramusinto, Gunawan Pria Utama, M.Anif	2021	Penelitian ini menggunakan algoritma kriptografi Blowfish untuk mengenkripsi file audio hasil rapat di PT. Asuransi Central Asia. Data audio yang digunakan berasal dari	Aplikasi berhasil mengenkripsi file audio hingga ukuran maksimum 120 MB. Rata-rata waktu proses enkripsi adalah 37 detik, sementara dekripsi membutuhkan 52,2 detik.	Algoritma Blowfish terbukti efektif untuk mengamankan data audio. Aplikasi yang dikembangkan tidak hanya memenuhi kebutuhan keamanan tetapi juga diterima dengan baik oleh pengguna.

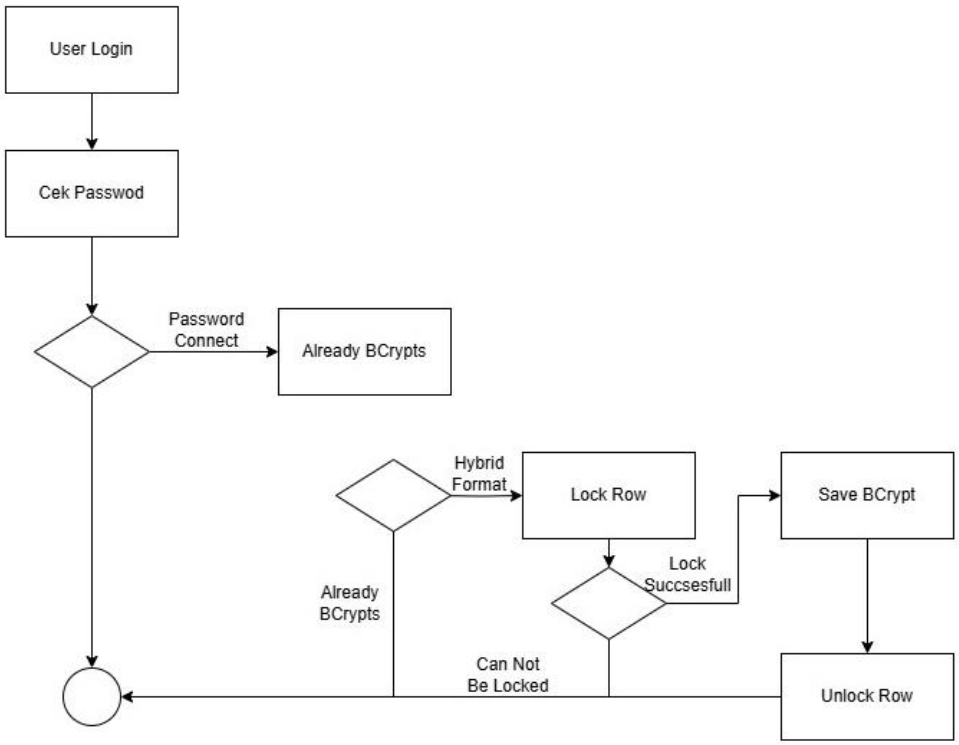
			notulen rapat tahun 2021. Proses meliputi analisis kebutuhan data, implementasi algoritma Blowfish dalam aplikasi berbasis Visual Basic 6.0		
Watermarking File Pdf Menggunakan Metode One-To-One Mapping(Sitohang, 2022)	Jefri Andreas Sitohang	2022	Penelitian ini menggunakan metode one-to-one mapping untuk menyisipkan watermark berupa citra ke dalam file PDF. Metode ini memetakan nilai piksel dari gambar asli dan watermark untuk	Hasil penelitian menunjukkan bahwa metode one-to-one mapping dapat diimplementasikan dengan baik untuk watermarking file PDF. Penyisipan watermark dilakukan pada file PDF bab pertama skripsi penulis dengan watermark berupa logo universitas. Watermark terlihat jelas pada PDF namun tetap menjaga kualitas file.	Metode one-to-one mapping terbukti efektif untuk menyisipkan dan mengekstrak watermark pada file PDF. Proses ini menjaga kualitas dokumen dan memberikan perlindungan hak cipta yang dapat dipertanggungjawabkan. Penelitian ini menunjukkan bahwa metode ini cocok untuk mengamankan dokumen digital tanpa mengurangi kualitas asli dokumen.

IMPLEMENTASI SISTEM STEGANOGRAFI CITRA DENGAN METODE SUBTITUSI LSB (LEAST SIGNIFICANT BIT)(Veriarinal & Wanandi, 2024)	Veriarinal, Reza Wanandi	2024	menyisipkan tanda tertentu tanpa mengubah kualitas file. Penelitian ini mengimplementasikan metode Least Significant Bit (LSB) dalam steganografi citra digital menggunakan MATLAB. Proses kerja sistem melibatkan encoding dan decoding pesan pada citra digital dengan memanfaatkan bit paling tidak signifikan (LSB)	Hasil penelitian menunjukkan bahwa metode LSB dapat menyisipkan pesan dalam citra digital dengan kualitas yang cukup baik. Nilai PSNR untuk berbagai panjang karakter pesan menunjukkan tingkat keberhasilan yang tinggi, dengan derau minimal pada citra hasil. Misalnya, pada gambar beresolusi 1200×675 dengan panjang pesan hingga 30.000 karakter, PSNR mencapai 63,965 dB, sedangkan nilai MSE sangat kecil, yaitu 0,034.	Penelitian ini menyimpulkan bahwa metode LSB efektif untuk menyisipkan pesan rahasia ke dalam citra digital tanpa mengurangi kualitas visual secara signifikan. Nilai PSNR yang tinggi dan MSE yang rendah menunjukkan bahwa hasil steganografi memiliki derau minimal. Namun, efisiensi waktu proses menjadi tantangan ketika pesan yang disisipkan semakin besar.

			untuk menyisipkan data. Evaluasi dilakukan pada empat file citra digital dengan format PNG32 yang memiliki ukuran dan resolusi berbeda.		
Teknik Steganograph yuntuk MenyisipkanPesan pada Sebuah Citra Menggunakan Metode Least Significant Bit(LSB)(Khuzaifi et al., 2022)	Ahmad Khuzaifi, Fauziah, Iskandar Fitri	2022	Penelitian ini menggunakan metode Least Significant Bit (LSB) untuk menyisipkan pesan rahasia ke dalam citra digital. Metode ini bekerja dengan memodifikasi bit terkecil dari piksel citra	Hasil penelitian menunjukkan bahwa metode LSB berhasil menyisipkan file teks berisi pesan rahasia ke dalam citra digital tanpa perubahan visual yang signifikan. Citra asli berukuran 56,9 KB setelah proses enkripsi menjadi 732 KB. Ukuran dimensi citra tetap sama, yaitu 500×500 piksel. Proses dekripsi juga berhasil mengekstraksi pesan rahasia yang disisipkan tanpa kehilangan informasi. Histogram citra asli dan citra watermark menunjukkan perbedaan yang kecil, menandakan perubahan hanya terjadi pada bit-bit terkecil yang tidak memengaruhi tampilan visual citra.	Penelitian ini menyimpulkan bahwa metode LSB efektif untuk menyisipkan pesan rahasia pada citra digital. Keuntungan metode ini adalah perubahan visual pada citra hasil hampir tidak terlihat, sementara pesan rahasia dapat disisipkan dan diekstraksi dengan baik. Namun, ukuran file citra meningkat setelah proses enkripsi.

digital untuk menyisipkan data pesan.

2.6 Flowchart Login



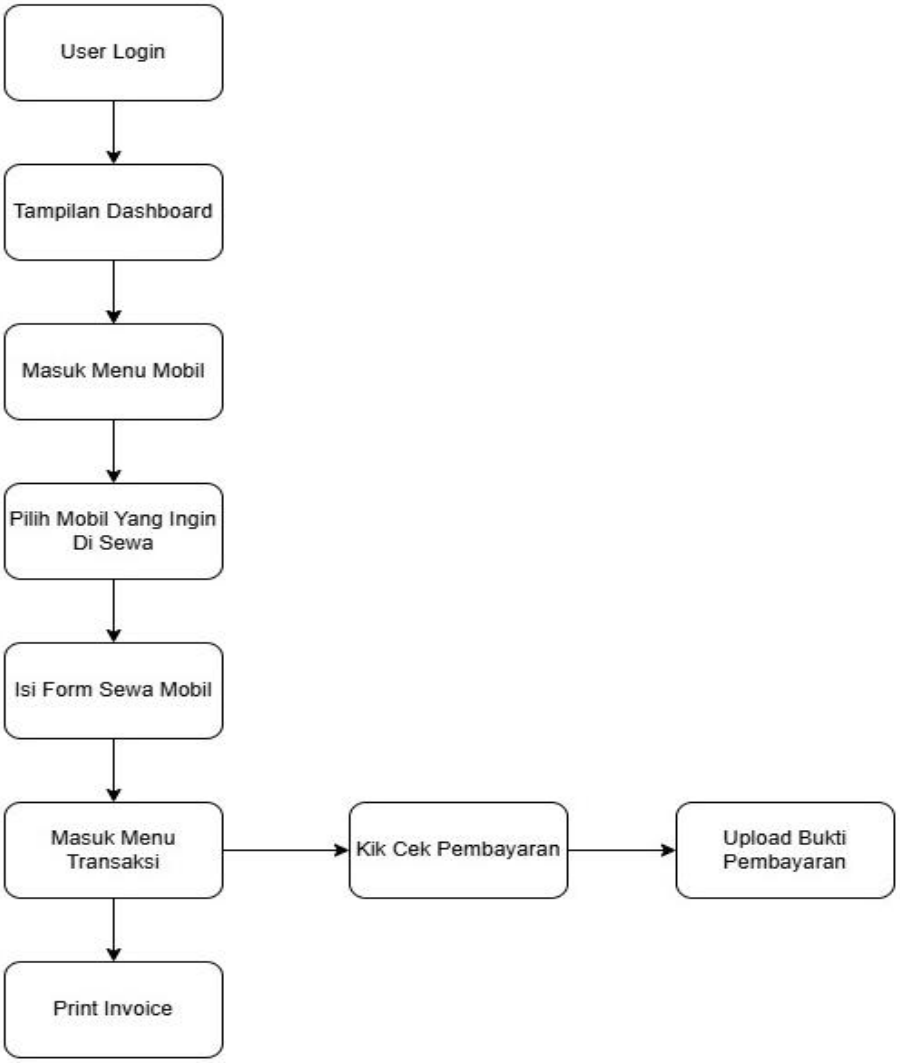
Gambar 5. Flowchart Login

Flowchart login diatas dijelaskan sebagai berikut:

- Memulai proses login.
- Masukkan username dan password.
- Sistem melakukan enkripsi terhadap password
- Jika username dan password yang dimasukkan valid maka akan langsung masuk ke dashboard customer/admin.
- Jika username/password salah maka akan muncul notifikasi username/password salah. Dan masukkan username & password Kembali hingga benar

E-ISSN: 2985-3532

2.7. Flowchart Sistem



Gambar 6. Flowchart Sistem

2.8 Alur Sistem

Alur dari sistem Rental Mobil Berbasis Web ini dimulai ketika pengguna melakukan login ke dalam sistem menggunakan username dan password. Password yang diinputkan kemudian di hashing menggunakan BCrypt. Jika username dan password valid maka pengguna diarahkan ke Dashboard yang menampilkan mobil yang disewakan, dan user bisa melihat dan memilih mobil mana yang akan disewa.

Ketika pengguna ingin melakukan transaksi mobil yang diinginkan, dan melakukan pembayaran melalui nomor yang tertera di sistem. Setelah pengguna selesai, mereka dapat mencetak invoice pembayaran dengan format file pdf dan dapat didownload serta disimpan pada perangkat pengguna. Pada file yang didownload terdapat watermark yang dapat digunakan

E-ISSN: 2985-3532

untuk melindungi informasi sensitif pada dokumen keuangan dengan menandai bahwa dokumen tersebut bersifat rahasia atau terbatas.

2.9 Cara Kerja BCrypt

- BCrypt memperkenalkan fungsi penguatan kata sandi. Jika kata sandi teks biasa terlalu pendek, kata sandi tersebut dapat dipanjangkan menjadi lebih panjang dan lebih rumit. Bcrypt menyediakan hingga 72 byte untuk kata sandi, meskipun umumnya, hingga 56 byte digunakan untuk menghasilkan hash 31 karakter. Hash kata sandi dapat mencapai hingga 23 byte dari hash 24 byte yang dihitung.

- Salt. Nilai salt acak berukuran 16-byte ditambahkan di depan kata sandi teks biasa. Salt kemudian di-hash, menghasilkan string 22 karakter yang ditempatkan di depan hash kata sandi.

- Faktor biaya. Biaya numerik ditambahkan di depan salt dan hash kata sandi, yang menunjukkan berapa banyak iterasi kata sandi yang dilakukan sebelum hash dibuat.

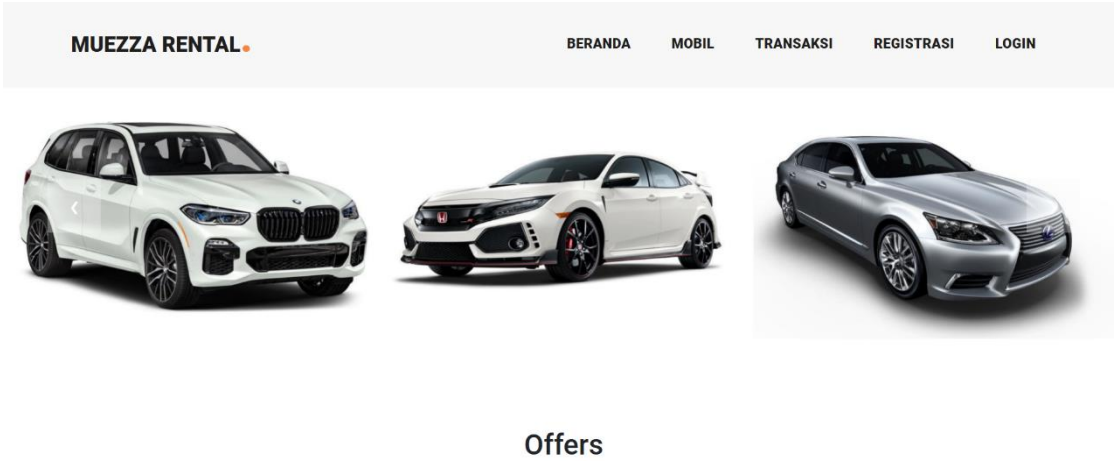
String hash kemudian diawali dengan pengidentifikasi algoritma hash bcrypt: $2a$, $2y$, atau $2b$.

```
            $this->load->view('ganti_password');
            $this->load->view('templates_admin/footer');
        } else {
            // Meng-hash password baru
            $hashed_password = password_hash(password: $pass_baru, algo: PASSWORD_BCRYPT);
            $data = array('password' => $hashed_password);
            $id = array('id_customer' => $this->session->userdata('id_customer'));

            // Update password di database
            $this->rental_model->update_password($id, $data, 'customer');
            $this->session->set_flashdata('pesan', '<div class="alert alert-success alert-dismissible fade show" role
            Password berhasil diupdate, silahkan login.
            <button type="button" class="close" data-dismiss="alert" aria-label="close">
                <span aria-hidden="true">&times;</span>
            </button></div>');
            redirect(uri: 'auth/login'); // Redirect ke halaman login
        }
    }

    // Validasi form login
    1 reference | 0 overrides
    public function _rules(): void {
        $this->form_validation->set_rules('username', 'Username', 'required');
        $this->form_validation->set_rules('password', 'Password', 'required');
    }
}
```

Gambar 7. Implementasi Hashing BCrypt

III. HASIL DAN PEMBAHASAN

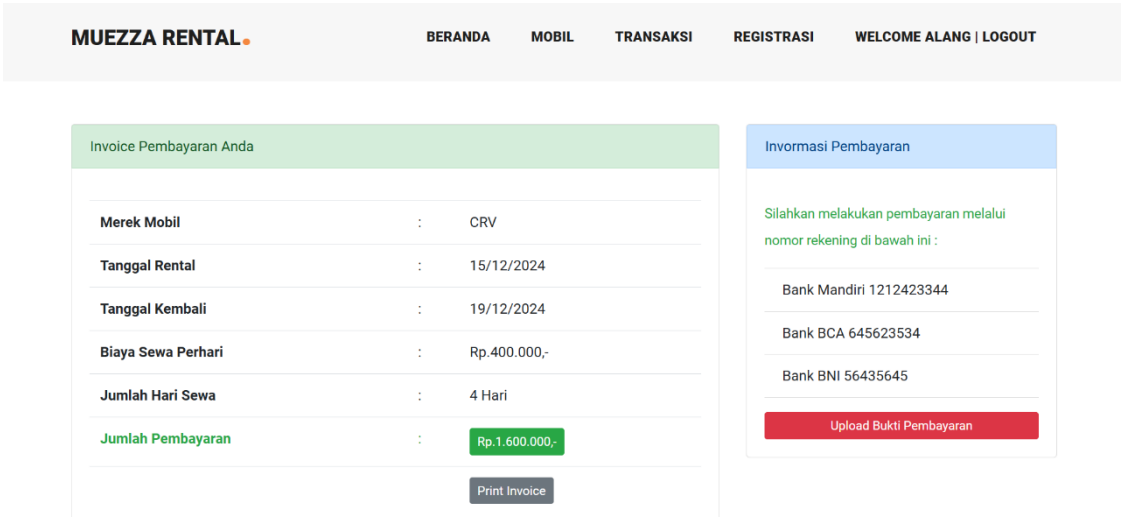
Gambar 8. Tampilan Form Login



Gambar 9. Tampilan Dashboard Customer

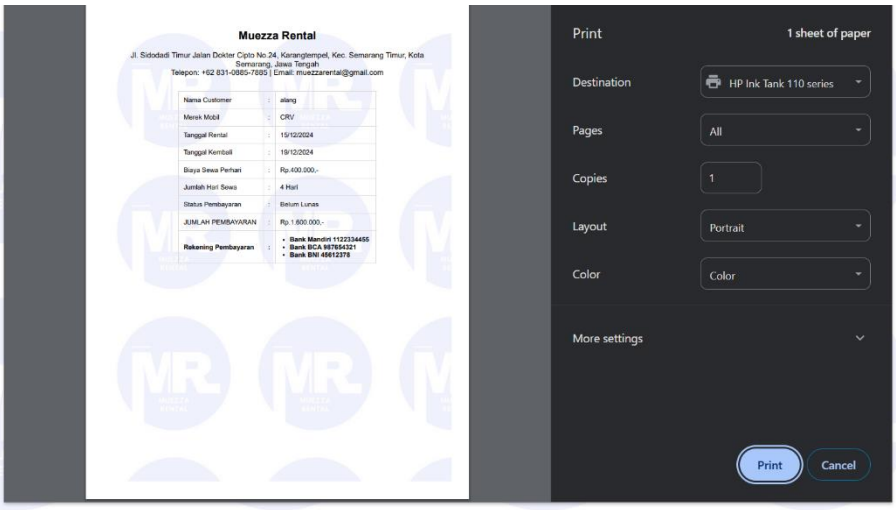
Dalam Tampilan Dashboard terdapat menu sebagai berikut :

- Mobil : Didalam menu Mobil terdapat beberapa pilihan mobil yang dapat di sewa.
- Transaksi : Di menu Transaksi terdapat data transaksi dan menu pembayaran.
- Registrasi : Menu Registrasi dapat digunakan untuk membuat akun.
- Login : Jika user sudah mempunyai akun maka dapat melakukan Login.

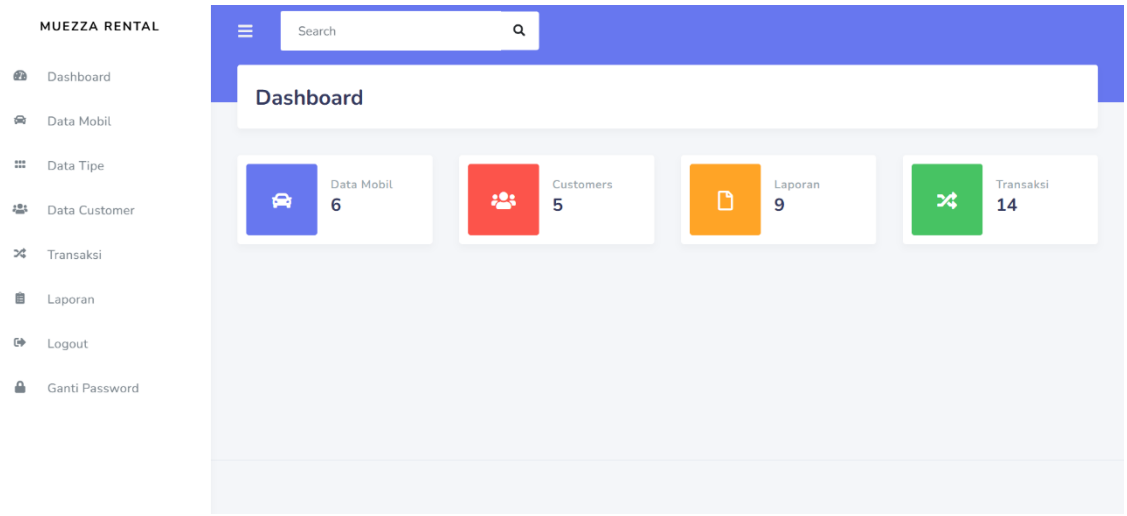


Gambar 10. Tampilan Pembayaran

Pada menu Pembayaran pengguna dapat melakukan pembayaran dengan cara click tombol Upload Bukti Pembayaran setelah pengguna melakukan upload bukti pembayaran, tunggu admin melakukan acc pembayaran. Pada menu pembayaran juga terdapat fitur Print Invoice.



Gambar 11. Tampilan Print Invoice Dengan Watermark



Gambar 12. Tampilan Dashboard Admin

Pada dashboard admin terdapat beberapa menu sebagai berikut :

- Data Mobil : Pada menu Data Mobil terdapat data - data mobil yang tersedia.
- Data Type : Di menu Data Type terdapat type - type mobil yang dapat di sewa di Muezza Rental.
- Data Customer : Pada menu Data Customer berisi data - data customer.

- Transaksi : Di menu Transaksi admin dapat melihat transaksi yang dilakukan oleh customer
- Laporan : Pada menu Laporan Admin Dapat melihat dan print laporan transaksi
- Ganti Pasword : Admin dapat mengganti password baru pada menu Ganti Password

-

IV. KESIMPULAN

Dengan mengutamakan efisiensi dan keamanan data pengguna, proyek ini menghasilkan sistem rental mobil berbasis web. Hashing Blowfish digunakan oleh sistem untuk melindungi kata sandi pengguna, dan mekanisme salt dan iterasi biaya memperlambat serangan brute force. Selain itu, sistem menempelkan watermark pada dokumen keuangan untuk mencegah data diubah atau didistribusikan secara tidak sah.

sistem membuat proses pengguna menjadi lebih mudah, mulai dari pendaftaran hingga pembayaran, dan memberikan keamanan tambahan yang mendukung kepercayaan pengguna. Selain itu, fitur administrator memungkinkan pengelolaan data seperti mobil, pelanggan, transaksi, dan laporan secara efektif. Dengan antarmuka yang sederhana namun berfungsi, sistem ini mampu meningkatkan efisiensi operasional sekaligus melindungi data pelanggan dengan baik.

V. UCAPAN TERIMA KASIH (Jika ada)

Jika makalah merupakan hasil penelitian yang didanai oleh sebuah *grant*, sebutkan nama *grant* yang diperoleh lengkap dengan nomor *project*-nya.

VI. REFERENSI

Amsari, F. D., Prasetyo, B. H., Pramusinto, W., Utama, G. P., & Anif, M. (2021). Pengamanan File Audio Menggunakan Algoritma Kriptografi Blowfish Dan Pengujian UAT. *Prosiding SISFOTEK*, *5*(1), 262–269.

Khuzaifi, A., Fauziah, F., & Fitri, I. (2022). Teknik Steganography untuk Menyisipkan Pesan pada Sebuah Citra Menggunakan Metode Least Significant Bit (LSB). *Jurnal JTIK (Jurnal Teknologi Informasi Dan Komunikasi)*, *6*(3), 417–423.

Naufal Yafie, H. (2020). *Analisis Penggunaan Fungsi Hash BCrypt untuk Keamanan Kata Sandi*.

Rosmiyati, J., & Mulyana, T. M. S. (2018). Watermark Dengan Gabungan Steganografi Dan Visible Watermarking. *Jurnal Algoritma, Logika Dan Komputasi*, *1*(1).

Sitohang, J. A. (2022). Watermarking File Pdf Menggunakan Metode One-To-One Mapping. *Resolusi: Rekayasa Teknik Informatika Dan Informasi*, *2*(3), 106–109.

Syafar, F., Husain, H., Suhaeb, S., & Ida, P. (2023). Blowfish Advanced CS Untuk Solusi Keamanan Sistem Komputer Sekolah. *Vokatek: Jurnal Pengabdian Masyarakat*, 353–361.

Veriarinal, V., & Wanandi, R. (2024). IMPLEMENTASI SISTEM STEGANOGRAFI CITRA DENGAN METODE SUBTITUSI LSB (LEAST SIGNIFICANT BIT). *Kohesi: Jurnal Sains Dan Teknologi*, *2*(11), 10–20.