Journal of Computer Science and Technology
JCS-TECH Vol.6, No.1, Mei 2026, PP. 9-15
e-ISSN 2808-9677, p-ISSN 2809-1140

IMPLEMENTASI TEKNIK DATA MASKING UNTUK PERLINDUNGAN DATA PELANGGAN PADA WEBSITE E-COMMERCE

Tia Agustina Widyastuti[1], Yudo Bismo Utomo[2*], Harso Kurniadi[3]
[1,2,3] Universitas Islam Kadiri, Kediri
[1]tiaagustina678@gmail.com, [2]yudobismo@uniska-kediri.ac.id, [3]harsokurniadi@uniska-kediri.ac.id

Abstrak

Keamanan data pelanggan menjadi aspek penting dalam pengelolaan website e-commerce karena sistem menyimpan informasi sensitif seperti nomor telepon, alamat email, dan riwayat transaksi. Apabila data tersebut tidak dilindungi dengan baik, maka berpotensi menimbulkan kebocoran data serta penyalahgunaan oleh pihak yang tidak berwenang. Penelitian ini bertujuan untuk mengimplementasikan teknik data masking sebagai solusi perlindungan data pelanggan pada website e-commerce. Metode penelitian yang digunakan adalah Action Research dengan tahapan perencanaan, tindakan, observasi, dan evaluasi. Teknik data masking diterapkan dengan menyamarkan seluruh karakter data sensitif menggunakan simbol tertentu tanpa mengubah data asli pada basis data. Pengujian sistem dilakukan menggunakan Blackbox Testing dan User Acceptance Testing (UAT) terhadap 293 responden. Hasil penelitian menunjukkan seluruh fitur sistem berjalan sesuai kebutuhan, dengan nilai UAT sebesar 85,37% dalam kategori sangat baik. Penelitian ini berkontribusi pada pengembangan sistem keamanan informasi melalui penerapan teknik data masking sebagai metode perlindungan privasi pelanggan pada layanan digital berbasis website. Dengan demikian, sistem yang dikembangkan efektif dan layak diterapkan pada platform e-commerce untuk meningkatkan keamanan data pelanggan.

Kata Kunci: *Data Masking, Keamanan Data, Privasi Data, Website E-Commerce, Pelanggan.*

Abstract

Customer data security is an important aspect in managing e-commerce websites because such systems store sensitive information such as phone numbers, email addresses, and transaction histories. If not properly protected, this data may lead to breaches and misuse by unauthorized parties. This study aims to implement a data masking technique as a solution for protecting customer data on an e-commerce website. The research method used was Action Research, consisting of planning, action, observation, and evaluation stages. The data masking technique was applied by disguising all sensitive data characters using specific symbols without changing the original data stored in the database. System testing was conducted using Blackbox Testing and User Acceptance Testing (UAT) involving 293 respondents. The results showed that all system features functioned properly, with a UAT score of 85.37%, categorized as very good. This study contributes to the development of information security systems through the application of data masking as a method for protecting customer privacy in website-based digital services. Therefore, the developed system is effective and feasible to be implemented on e-commerce platforms to improve customer data security.

Keywords: *Data Masking, Data Security, Data Privacy, E-Commerce Website, Customer.*

1. Pendahuluan

Perkembangan teknologi informasi telah mendorong transformasi digital pada berbagai sektor usaha (Harto, B., Rukmana, A. Y., Subekti, R., Tahir, R., Waty, E., Situru, A. C., & Sepriano, S. (2023), termasuk perdagangan berbasis elektronik (e-commerce). Website e-commerce menjadi sarana penting bagi pelaku usaha dalam memasarkan produk (Meylano, N. H., Woda, Y. W. B., Mukin, D. P., Pereira, F. L., & Theresia, D. E. (2025), mengelola transaksi (Susanti, A., & Prabowo, D. W. (2017), serta membangun hubungan dengan pelanggan secara lebih efektif dan efisien. Melalui sistem berbasis website, pelanggan dapat melakukan pemesanan produk (Al-amin, N. K. P., & Mariana, N. (2022), memperoleh informasi produk (Sitorus, J. H. P., & Sakban, M. (2021), dan melakukan transaksi secara online (Yudianto, F., Annisaa'Firdaus, M.,

Susanto, F. A., & Herlambang, T. (2022). Namun, semakin meningkatnya penggunaan layanan digital juga diikuti oleh meningkatnya risiko keamanan data dan privasi pengguna.

Data pelanggan merupakan aset penting yang harus dijaga kerahasiaan dan keamanannya. Informasi seperti nomor telepon, alamat email, alamat pengiriman, dan riwayat transaksi termasuk kategori data sensitif yang berpotensi disalahgunakan apabila diakses oleh pihak yang tidak berwenang. Kebocoran data pelanggan dapat menimbulkan berbagai dampak negatif, seperti penyalahgunaan identitas (Erikha, A., & Hoesein, Z. A. (2025), penipuan digital (Aritonang, L. M., Zyetwill, Z., & Handayani, R. (2025), spam (Rahmawati, D., Aksana, M. D. A., & Mukaromah, S. (2023), hingga menurunnya tingkat kepercayaan pelanggan terhadap layanan yang diberikan (Putri, F. N. S., Utomo, Y. B., & Kurniadi, H. (2023). Oleh karena itu, perlindungan data pelanggan menjadi salah satu aspek utama dalam pengelolaan website e-commerce modern.

Permasalahan keamanan data pada website sering kali terjadi karena informasi sensitif ditampilkan secara langsung pada antarmuka sistem tanpa mekanisme perlindungan tambahan. Kondisi tersebut meningkatkan risiko terjadinya akses tidak sah, terutama ketika sistem digunakan oleh banyak pengguna atau administrator. Selain itu, tidak semua pelaku usaha, khususnya usaha kecil dan menengah, memiliki sumber daya yang memadai untuk menerapkan teknologi keamanan yang kompleks dan berbiaya tinggi. Dengan demikian, dibutuhkan solusi keamanan yang efektif, efisien, dan mudah diterapkan sesuai kebutuhan sistem.

Beberapa penelitian sebelumnya menunjukkan bahwa perlindungan data pada sistem informasi umumnya dilakukan melalui pendekatan enkripsi data, autentikasi pengguna, firewall, maupun keamanan jaringan. Pendekatan tersebut terbukti mampu meningkatkan keamanan sistem, namun dalam implementasinya sering memerlukan konfigurasi teknis yang lebih kompleks dan biaya pengelolaan tambahan. Di sisi lain, penelitian mengenai penerapan data masking sebagai perlindungan data pelanggan pada website e-commerce masih relatif terbatas, terutama pada usaha skala kecil dan menengah yang membutuhkan solusi praktis dan terjangkau.

Data masking merupakan teknik penyamaran data dengan cara menyembunyikan informasi sensitif pada tampilan sistem tanpa mengubah data asli yang tersimpan di dalam basis data (Salsabila, C. R., & Gunawan, D. (2026). Melalui teknik ini, data penting tetap terlindungi ketika ditampilkan kepada pengguna, sehingga risiko kebocoran informasi dapat diminimalkan. Teknik ini memiliki keunggulan dalam kemudahan implementasi, efisiensi sumber daya, serta tetap mempertahankan fungsi operasional sistem. Oleh karena itu, data masking dapat menjadi alternatif solusi keamanan data yang sesuai untuk platform e-commerce.

Penelitian ini mengusulkan implementasi teknik data masking untuk perlindungan data pelanggan pada website e-commerce dengan studi kasus pada platform Tani Maju Milenial. Data sensitif pelanggan seperti nomor telepon, alamat email, dan riwayat transaksi ditampilkan dalam bentuk tersamarkan menggunakan simbol tertentu, sementara data asli tetap tersimpan secara aman di dalam basis data. Pendekatan penelitian menggunakan metode Action Research yang meliputi tahapan perencanaan, tindakan, observasi, dan evaluasi agar solusi yang dikembangkan sesuai dengan kebutuhan nyata pengguna sistem.

Nilai keterbaruan (novelty) penelitian ini terletak pada penerapan teknik full data masking secara real-time untuk melindungi seluruh karakter data sensitif pelanggan pada website e-commerce. Berbeda dengan penelitian sebelumnya yang lebih berfokus pada perlindungan data melalui enkripsi dan keamanan jaringan, penelitian ini menekankan perlindungan privasi data pada sisi tampilan sistem dengan implementasi yang lebih ringan, praktis, dan mudah diterapkan. Pendekatan ini memberikan kontribusi dalam pengembangan sistem keamanan informasi, khususnya bagi pelaku usaha digital yang membutuhkan solusi perlindungan data pelanggan secara efektif dan terjangkau.

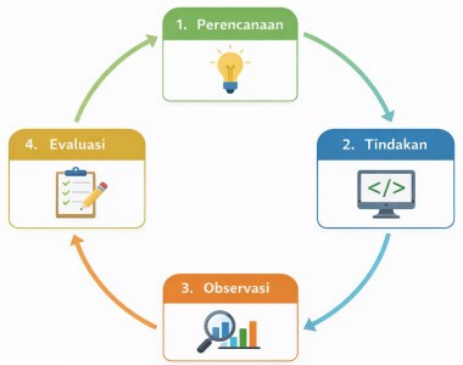
Berdasarkan uraian tersebut, penelitian ini bertujuan untuk mengimplementasikan teknik data masking serta mengevaluasi tingkat keberhasilan sistem dalam melindungi data pelanggan pada website e-commerce. Hasil penelitian diharapkan dapat menjadi referensi bagi pengembang sistem informasi dan pelaku usaha dalam meningkatkan keamanan data pelanggan melalui pendekatan yang sederhana namun efektif.

2. Metode Penelitian

Penelitian ini menggunakan metode Action Research, yaitu pendekatan penelitian yang berorientasi pada pemecahan masalah nyata melalui tindakan langsung secara sistematis untuk menghasilkan perbaikan pada suatu sistem (Utomo, Y. B., Pratomo, A. R., & Pradipta,

Journal of Computer Science and Technology
JCS-TECH Vol.6, No.1, Mei 2026, PP. 9-15
e-ISSN 2808-9677, p-ISSN 2809-1140

D. (2025). Metode ini dipilih karena sesuai dengan tujuan penelitian, yaitu meningkatkan keamanan data pelanggan pada website e-commerce melalui implementasi teknik data masking. Melalui pendekatan ini, peneliti dapat melakukan identifikasi masalah, penerapan solusi, pengamatan hasil, serta evaluasi secara berkelanjutan. Alur dari metode action research ditampilkan pada gambar 1 berikut.



Gambar 1. Alur Metode Action Research

Tahapan ini dilakukan secara berurutan agar solusi yang diterapkan dapat menjawab permasalahan sistem secara efektif. Tahapan dari metode action research antara lain sebagai berikut:

1. Perencanaan (*Planning*)
   Tahap ini dilakukan dengan mengidentifikasi permasalahan pada sistem yang berjalan, yaitu data pelanggan masih ditampilkan secara penuh sehingga berisiko menimbulkan kebocoran informasi. Selanjutnya dilakukan analisis kebutuhan sistem serta perancangan solusi keamanan menggunakan teknik data masking.
2. Tindakan (*Action*)
   Pada tahap ini dilakukan implementasi teknik data masking ke dalam website e-commerce. Sistem dirancang agar data sensitif pelanggan ditampilkan dalam bentuk tersamarkan menggunakan simbol bintang (*) tanpa mengubah data asli yang tersimpan di dalam basis data.
3. Observasi (*Observation*)
   Tahap observasi dilakukan dengan mengamati hasil implementasi sistem, khususnya pada keberhasilan proses masking, tampilan antarmuka, dan kestabilan fungsi sistem selama digunakan.
4. Evaluasi (*Evaluation*)
   Tahap evaluasi dilakukan melalui pengujian sistem untuk menilai efektivitas solusi yang diterapkan. Hasil evaluasi menjadi dasar perbaikan dan penyempurnaan sistem keamanan data.

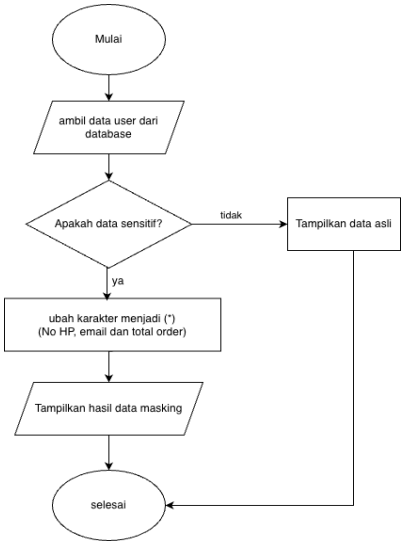
2.1. Teknik Pengumpulan Data

Data penelitian diperoleh melalui beberapa teknik berikut:

1. Observasi, yaitu mengamati kondisi sistem website yang sedang berjalan.
2. Wawancara, dilakukan kepada pengelola sistem untuk mengetahui kebutuhan keamanan data.
3. Studi Literatur, dilakukan dengan mempelajari jurnal, buku, dan penelitian terdahulu yang relevan dengan keamanan data dan data masking.

2.2. Teknik Data Masking

Teknik yang diterapkan dalam penelitian ini adalah teknik data masking, yaitu metode penyamaran data dengan menyembunyikan seluruh karakter data sensitif menggunakan simbol tertentu. Data asli tetap tersimpan di dalam basis data, sedangkan data yang ditampilkan kepada pengguna telah disamarkan. Proses masking dilakukan secara dinamis saat data ditampilkan pada sistem. Langkah algoritma divisualisasikan sebagai berikut:



Gambar 2. Algoritma Teknik Data Masking

Gambar tersebut merupakan flowchart prosedur algoritma teknik data masking yang menggambarkan alur sistem dalam melindungi data sensitif pengguna pada website. Proses dimulai dari pengambilan data user dari database, kemudian sistem melakukan identifikasi apakah data yang diakses termasuk kategori sensitif. Apabila data tidak sensitif, maka sistem akan langsung menampilkan data asli kepada pengguna. Namun, apabila data termasuk sensitif, seperti nomor telepon, email, dan total pesanan, maka sistem akan melakukan proses penyamaran dengan mengubah karakter data menjadi simbol bintang (*). Setelah proses masking selesai, sistem menampilkan hasil data yang telah disamarkan. Seluruh proses

kemudian berakhir pada tahap selesai. Flowchart ini menunjukkan bahwa teknik data masking diterapkan secara selektif hanya pada data yang bersifat sensitif, sehingga keamanan dan privasi data pelanggan dapat lebih terjaga.

2.3. Pengujian Sistem

Pengujian sistem dilakukan menggunakan dua metode, yaitu:

1. Blackbox Testing
   Blackbox Testing digunakan untuk menguji fungsi sistem berdasarkan kesesuaian input dan output tanpa melihat struktur kode program (Bachrudin, N. M., Utomo, Y. B., & Kurniasari, I. (2023). Pengujian meliputi fitur login, tampilan data pelanggan, proses masking, serta navigasi sistem.
2. User Acceptance Testing (UAT)
   User Acceptance Testing (UAT) digunakan untuk mengetahui tingkat penerimaan pengguna terhadap sistem yang dikembangkan (Putri, D., Afriansyah, R., & Prayesy, P. A. (2025). Pengujian dilakukan terhadap 293 responden yang terdiri dari pengguna sistem. Instrumen penilaian menggunakan kuesioner dengan empat aspek, yaitu Functionality; Reliability; Usability; Efficiency. Setiap jawaban responden diukur menggunakan skala penilaian, kemudian dihitung dalam bentuk persentase untuk mengetahui tingkat kelayakan sistem.

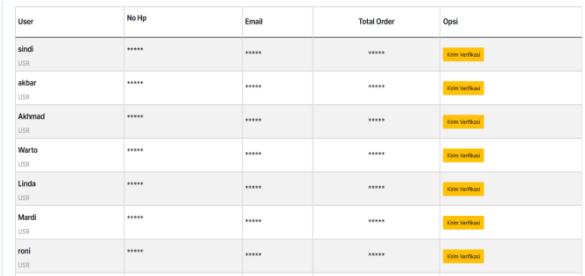
3. Hasil dan Pembahasan

Bagian ini menyajikan hasil implementasi teknik data masking pada website e-commerce serta pembahasan terhadap pengujian sistem yang telah dilakukan. Hasil penelitian difokuskan pada penerapan teknik data masking, pengujian fungsional sistem menggunakan Blackbox Testing, serta evaluasi tingkat penerimaan pengguna melalui User Acceptance Testing (UAT). Pembahasan dilakukan untuk mengetahui efektivitas sistem dalam melindungi data sensitif pelanggan dan kelayakan penerapannya pada layanan digital berbasis website.

3.1. Hasil Teknik Data Masking

Implementasi teknik data masking dilakukan pada website e-commerce untuk meningkatkan perlindungan data pelanggan yang tersimpan di dalam sistem. Penerapan fitur ini difokuskan pada data yang bersifat sensitif, seperti nomor telepon, alamat email, dan total pesanan pelanggan. Sebelum implementasi dilakukan, data pelanggan masih ditampilkan secara lengkap pada halaman admin maupun halaman pengelolaan data, sehingga berpotensi menimbulkan risiko kebocoran informasi apabila diakses oleh pihak yang tidak berwenang.

Setelah teknik data masking diterapkan, sistem secara otomatis menyamarkan data sensitif saat informasi ditampilkan pada antarmuka website. Proses masking dilakukan tanpa mengubah data asli yang tersimpan di dalam basis data, sehingga integritas data tetap terjaga. Informasi yang disamarkan ditampilkan dalam bentuk simbol bintang (*) agar isi data tidak dapat dibaca secara langsung oleh pengguna yang tidak memiliki hak akses tertentu, seperti yang ditunjukkan pada gambar 3 berikut.



Gambar 3. Hasil Teknik Data Masking

Implementasi teknik data masking pada penelitian ini diterapkan secara selektif sesuai jenis data. Nomor telepon pelanggan ditampilkan dalam bentuk tersamarkan, alamat email disembunyikan menggunakan simbol tertentu, dan total pesanan pelanggan juga tidak ditampilkan secara utuh. Dengan mekanisme tersebut, data pelanggan tetap terlindungi meskipun halaman sistem diakses oleh pengguna lain.

Penerapan teknik data masking memberikan dampak positif terhadap keamanan sistem, karena informasi sensitif tidak lagi terlihat secara terbuka pada tampilan website. Selain itu, fitur ini tidak memengaruhi proses operasional sistem maupun kinerja website, sehingga dapat diterapkan sebagai solusi keamanan yang ringan, efektif, dan mudah diimplementasikan pada platform e-commerce.

3.2. Hasil Blackbox Testing

Pengujian sistem dilakukan menggunakan metode Blackbox Testing untuk mengetahui apakah setiap fitur pada website e-commerce dapat berjalan sesuai fungsi yang telah dirancang. Pengujian dilakukan dengan memeriksa hubungan antara masukan (input) yang diberikan pengguna dengan keluaran (output) yang dihasilkan sistem tanpa meninjau kode program secara langsung. Fitur yang diuji meliputi proses login, tampilan data pelanggan, penerapan teknik data masking, navigasi menu, serta proses logout.

Hasil pengujian menunjukkan bahwa seluruh fitur utama pada sistem dapat berjalan dengan baik, seperti yang ditunjukkan pada tabel 1. Setiap fungsi yang diuji mampu menghasilkan keluaran sesuai kebutuhan pengguna, sehingga sistem dinilai siap digunakan pada tahap pengujian lanjutan.

Tabel 1. Hasil Blackbox Testing

No	Fitur yang diuji	Hasil yang diharapkan	Status
1	Login	Jika data login benar, sistem menampilkan dashboard. Jika data login salah, sistem menampilkan pesan gagal login.	Berfungsi
2	Data pelanggan	Sistem menampilkan data pelanggan	Berfungsi
3	Teknik data masking	Sistem menampilkan nomor telepon, email, dan total pesanan dalam bentuk simbol bintang (****)	Berfungsi
4	Navigasi menu	Perpindahan halaman sesuai menu yang dipilih	Berfungsi
5	Logout	Sistem keluar dari sesi pengguna	Berfungsi

Berdasarkan Tabel 1, seluruh fitur yang diuji menunjukkan status berfungsi sesuai skenario yang diberikan. Sistem mampu memvalidasi data login, menampilkan informasi pelanggan, menjalankan teknik data masking secara otomatis, serta merespons navigasi menu dan proses logout dengan baik. Dengan demikian, website e-commerce dinyatakan layak untuk dilanjutkan pada tahap pengujian pengguna menggunakan User Acceptance Testing (UAT).

3.3. Hasil User Acceptance Testing (UAT)

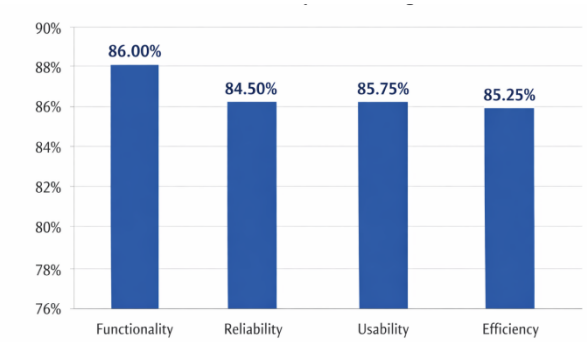
Pengujian User Acceptance Testing (UAT) dilakukan untuk mengetahui tingkat penerimaan pengguna terhadap sistem yang telah dikembangkan. Pengujian ini bertujuan menilai apakah website e-commerce dengan penerapan teknik data masking telah memenuhi kebutuhan pengguna dari sisi fungsi, kemudahan penggunaan, keandalan, dan efisiensi sistem. Responden yang terlibat dalam pengujian ini berjumlah 293 orang yang merupakan pengguna sistem.

Instrumen pengujian menggunakan kuesioner dengan skala penilaian yang terdiri dari empat aspek utama, yaitu Functionality, Reliability, Usability, dan Efficiency. Setiap responden memberikan penilaian terhadap sistem berdasarkan pengalaman penggunaan selama proses uji coba.

Berdasarkan hasil pengolahan data kuesioner, diperoleh nilai persentase pada masing-masing aspek sebagaimana ditunjukkan pada Tabel 2 berikut.

Tabel 2. Hasil User Acceptance Testing

No	Aspek Penilaian	Persentase
1	Functionality	86,00%
2	Reliability	84,50%
3	Usability	85,75%
4	Efficiency	85,25%
	Rata-Rata	85,37%



Gambar 4. Grafik Hasil User Acceptance Testing

Berdasarkan Tabel 2 dan Gambar 4, aspek Functionality memperoleh nilai tertinggi sebesar 86,00%, yang menunjukkan bahwa fitur-fitur pada sistem telah berjalan sesuai kebutuhan pengguna. Aspek Reliability memperoleh nilai 84,50%, yang menunjukkan bahwa sistem mampu beroperasi secara stabil selama digunakan. Selanjutnya, aspek Usability memperoleh nilai 85,75%, yang menandakan bahwa sistem mudah dipahami dan digunakan oleh pengguna. Adapun aspek Efficiency memperoleh nilai 85,25%, yang menunjukkan bahwa sistem mampu memberikan kinerja yang baik dengan waktu respons yang memadai.

Secara keseluruhan, nilai rata-rata UAT sebesar 85,37% berada pada kategori sangat baik, sehingga dapat disimpulkan bahwa sistem yang dikembangkan telah diterima dengan baik

oleh pengguna. Hasil ini menunjukkan bahwa penerapan teknik data masking tidak mengganggu kenyamanan penggunaan sistem, melainkan tetap mampu menjaga keamanan data pelanggan secara efektif.

3.4. Pembahasan

Hasil penelitian menunjukkan bahwa penerapan teknik data masking pada website e-commerce mampu meningkatkan perlindungan data pelanggan tanpa mengganggu fungsi utama sistem. Berdasarkan hasil implementasi, data sensitif seperti nomor telepon, alamat email, dan total pesanan berhasil disamarkan menggunakan simbol bintang (*), sehingga informasi penting tidak dapat dilihat secara langsung oleh pihak yang tidak berwenang. Kondisi ini menunjukkan bahwa teknik data masking dapat menjadi solusi praktis dalam menjaga privasi pelanggan pada layanan digital berbasis website.

Berdasarkan hasil Blackbox Testing, seluruh fitur utama sistem menunjukkan status berfungsi sesuai rancangan. Proses login, tampilan data pelanggan, penerapan masking, navigasi menu, serta logout dapat berjalan dengan baik. Hal ini membuktikan bahwa penambahan fitur keamanan melalui teknik data masking tidak menurunkan performa maupun mengganggu proses operasional website. Dengan demikian, sistem tetap dapat digunakan secara normal meskipun telah ditambahkan mekanisme perlindungan data.

Selanjutnya, hasil User Acceptance Testing (UAT) memperoleh nilai rata-rata sebesar 85,37% dengan kategori sangat baik. Nilai tersebut menunjukkan bahwa pengguna dapat menerima sistem dengan baik dari aspek fungsi, keandalan, kemudahan penggunaan, dan efisiensi. Tingginya tingkat penerimaan pengguna mengindikasikan bahwa penerapan teknik data masking tidak menimbulkan kesulitan dalam penggunaan sistem, sehingga fitur keamanan yang diterapkan tetap memberikan kenyamanan bagi pengguna.

Temuan penelitian ini memperlihatkan bahwa perlindungan data tidak selalu harus menggunakan teknologi yang kompleks dan berbiaya tinggi. Teknik data masking dapat diterapkan sebagai solusi yang lebih ringan, mudah diimplementasikan, dan sesuai bagi pelaku usaha kecil maupun menengah yang menggunakan website e-commerce. Selain menjaga keamanan informasi pelanggan, teknik ini juga membantu meningkatkan kepercayaan pengguna terhadap layanan digital yang disediakan.

Secara keseluruhan, penelitian ini memberikan kontribusi pada pengembangan sistem keamanan informasi, khususnya dalam penerapan teknik data masking pada website e-commerce. Hasil penelitian membuktikan bahwa teknik data masking efektif diterapkan untuk melindungi data pelanggan, menjaga fungsi sistem tetap optimal, serta memperoleh tingkat penerimaan pengguna yang tinggi. Dengan demikian, teknik ini layak direkomendasikan sebagai salah satu metode perlindungan data pada platform digital berbasis website.

4. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa penerapan teknik data masking pada website e-commerce berhasil meningkatkan perlindungan data pelanggan, khususnya pada informasi sensitif seperti nomor telepon, alamat email, dan total pesanan. Teknik ini mampu menyamarkan data pada tampilan sistem tanpa mengubah data asli yang tersimpan di dalam basis data, sehingga keamanan dan integritas data tetap terjaga.

Hasil Blackbox Testing menunjukkan bahwa seluruh fitur utama sistem dapat berjalan dengan baik sesuai fungsi yang dirancang, sedangkan hasil User Acceptance Testing (UAT) terhadap 293 responden memperoleh nilai rata-rata sebesar 85,37% dengan kategori sangat baik. Hal tersebut menunjukkan bahwa sistem diterima dengan baik oleh pengguna dari aspek fungsi, keandalan, kemudahan penggunaan, dan efisiensi.

Secara keseluruhan, penelitian ini membuktikan bahwa teknik data masking merupakan solusi yang efektif, ringan, dan mudah diterapkan untuk meningkatkan keamanan data pelanggan pada website e-commerce. Penelitian selanjutnya dapat mengembangkan teknik masking yang lebih adaptif atau mengombinasikannya dengan metode keamanan lain agar perlindungan data menjadi lebih optimal.

5. Daftar Pustaka

Harto, B., Rukmana, A. Y., Subekti, R., Tahir, R., Waty, E., Situru, A. C., & Sepriano, S. (2023). Transformasi bisnis di era digital: Teknologi informasi dalam mendukung transformasi bisnis di era digital. PT. Sonpedia Publishing Indonesia.

Meylano, N. H., Woda, Y. W. B., Mukin, D. P., Pereira, F. L., & Theresia, D. E. (2025). Penerapan metode requirement engineering dalam pengembangan website e-commerce sebagai media promosi dan pemasaran pada kelompok UMKM tenun ikat. Jurnal Indonesia:

Manajemen Informatika Dan Komunikasi, 6(1), 240–251.

Susanti, A., & Prabowo, D. W. (2017). E-commerce pada toko my digital. Jurnal Penelitian Dosen FIKOM (UNDA), 4(1).

Al-amin, N. K. P., & Mariana, N. (2022). Sistem Informasi Penjualan Sparepart Motor Pada NOPNOPPART Berbasis Website. Elkom: Jurnal Elektronika Dan Komputer, 15(1), 180–188.

Sitorus, J. H. P., & Sakban, M. (2021). Perancangan Sistem Informasi Penjualan Berbasis Web Pada Toko Mandiri 88 Pematangsiantar. Jurnal Bisantara Informatika, 5(2), 12–24.

Yudianto, F., Annisaa'Firdaus, M., Susanto, F. A., & Herlambang, T. (2022). Perancangan Sistem Informasi Penjualan Toko Online Galeri Nada Berbasis Website. Remik: Riset Dan E-Jurnal Manajemen Informatika Komputer, 6(3), 575–584.

Erikha, A., & Hoesein, Z. A. (2025). Strategi pencegahan kebocoran data pribadi melalui peran Kominfo dan gerakan Siberkreasi dalam edukasi digital. Jurnal Retentum, 4(1), 48–64.

Aritonang, L. M., Zyetwill, Z., & Handayani, R. (2025). Analisis Hukum terhadap Kebocoran Data Pribadi dan Penyalahgunaan Identitas dalam Perbankan Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Ranah Research: Journal of Multidisciplinary Research and Development, 7(5), 3146–3158.

Rahmawati, D., Aksana, M. D. A., & Mukaromah, S. (2023). Privasi dan keamanan data di media sosial: dampak negatif dan strategi pencegahan. Prosiding Seminar Nasional Teknologi Dan Sistem Informasi, 3(1), 571–580.

Putri, F. N. S., Utomo, Y. B., & Kurniadi, H. (2023). Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui Kali Linux. Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi), 7(1), 52–59.

Salsabila, C. R., & Gunawan, D. (2026). IMPLEMENTASI ALGORITMA FHSAR DALAM MENYEMBUNYIKAN ATURAN ASOSIASI SENSITIF PADA DATASET TRANSAKSI. Rabit: Jurnal Teknologi Dan Sistem Informasi Univrab, 11(1), 743–754.

Utomo, Y. B., Pratomo, A. R., & Pradipta, D. (2025). RANCANG BANGUN SISTEM PENJADWALAN BIMBINGAN TUGAS AKHIR DENGAN PENDEKATAN CRM BERBASIS WEBSITE. Jurnal Sistem Informasi, Teknologi Informatika Dan Komputer, 16(1), 27–32.

Bachrudin, N. M., Utomo, Y. B., & Kurniasari, I. (2023). Perancangan Aplikasi E-Archive Untuk Penyimpanan Laporan Tugas Akhir (Studi Kasus: Fakultas Teknik Uniska Kediri).

Putri, D., Afriansyah, R., & Prayesy, P. A. (2025). Implementasi User Acceptance Testing (UAT) Pada Pengujian Sistem Informasi Akademik dan Keuangan Santri. TeIKa, 15(2), 1–15.