JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Analisis Keamanan Data Pengguna pada Platform E-commerce: Studi Kasus Kebocoran Data Tokopedia 2020

Naila Zafira [1], Nabila Aisyahara [2], Cut Aidila Safriana[3], Rofli[4] , Hafizatunnisa[5]
[1,2,3,4,5]Universitas Malikussaleh, Indonesia
[1]naila.240170088@mhs.unimal.ac.id, [2]nabila.240170104@mhs.unimal.ac.id, [3]cut.240170109@mhs.unimal.ac.id,
[4]rofli.240170112@mhs.unimal.ac.id, [5]hafizatunnisa.240170131@mhs.unimal.ac.id

ABSTRACT

The rapid growth of e-commerce platforms has increased the collection and processing of users' personal data, which consequently raises security risks. One of the most significant incidents in Indonesia was the Tokopedia data breach in 2020. This study aims to analyze user data security issues on e-commerce platforms through a case study of the Tokopedia data breach. The research method uses a descriptive qualitative approach based on literature review and secondary data analysis. The results indicate that data breaches are influenced not only by technical vulnerabilities but also by weaknesses in data governance and security management. This study also reviews the incident from a legal perspective based on Indonesia's Personal Data Protection Law. The findings are expected to contribute to improving data security practices on e-commerce platforms.

Kata Kunci/ Keywords:
data security, e-commerce, data breach, Tokopedia, personal data protection

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di Indonesia telah mendorong pertumbuhan pesat industri *e-commerce*. Platform perdagangan elektronik kini menjadi tulang punggung ekonomi digital yang memfasilitasi jutaan transaksi setiap harinya. Seiring dengan peningkatan volume transaksi tersebut, pengumpulan dan pemrosesan data pribadi pengguna juga meningkat secara signifikan. Data pengguna, yang mencakup informasi sensitif seperti identitas pribadi, kredensial akun, dan riwayat transaksi, menjadi aset yang sangat berharga namun sekaligus rentan terhadap berbagai ancaman keamanan siber.

Keamanan sistem komputer, khususnya dalam konteks *e-commerce*, memegang peranan vital untuk menjamin kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data. Namun, meskipun berbagai mekanisme keamanan telah diterapkan, insiden kebocoran data (*data breach*) masih kerap terjadi. Salah satu insiden keamanan siber terbesar yang pernah terjadi di Indonesia adalah kasus kebocoran data pada platform Tokopedia pada tahun 2020. Dalam insiden ini, jutaan data pengguna dilaporkan telah diretas dan diperjualbelikan oleh pihak yang tidak bertanggung jawab, yang menimbulkan kekhawatiran besar mengenai privasi dan keamanan data di Indonesia.

Kasus ini menyoroti bahwa ancaman terhadap keamanan data tidak hanya bersifat teknis, tetapi juga berkaitan dengan tata kelola dan manajemen keamanan. Penerapan teknik kriptografi seperti fungsi *hash* untuk pengamanan kata sandi, *Message Authentication Code* (MAC) untuk integritas data, serta tanda tangan digital (*digital signature*) menjadi standar yang harus dievaluasi efektivitasnya dalam menghadapi serangan modern.

Penelitian ini bertujuan untuk menganalisis keamanan data pengguna pada platform *e-commerce* melalui studi kasus kebocoran data Tokopedia tahun 2020. Analisis akan dilakukan dengan meninjau insiden tersebut berdasarkan prinsip keamanan CIA Triad dan mengevaluasi penerapan mekanisme kriptografi yang ada. Melalui pendekatan kualitatif deskriptif, penelitian ini diharapkan dapat memberikan gambaran mengenai celah keamanan yang ada serta memberikan rekomendasi langkah-langkah mitigasi untuk mencegah terulangnya insiden serupa di masa mendatang, guna meningkatkan kepercayaan pengguna terhadap ekosistem ekonomi digital di Indonesia.

TINJAUAN PUSTAKA

Keamanan Sistem Komputer

Keamanan sistem komputer merupakan serangkaian upaya dan mekanisme yang diterapkan untuk melindungi sistem komputer, jaringan, dan data dari berbagai ancaman yang dapat menyebabkan kerusakan, pencurian, maupun akses yang tidak sah. Keamanan sistem komputer bertujuan untuk memastikan bahwa informasi yang tersimpan dan diproses dalam suatu sistem tetap terjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaannya (availability).

Ancaman terhadap keamanan sistem komputer dapat berasal dari berbagai sumber, baik internal maupun eksternal, seperti malware, serangan peretas, kesalahan pengguna, maupun kelemahan pada sistem itu sendiri. Oleh

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

karena itu, keamanan sistem komputer tidak hanya berfokus pada perlindungan perangkat keras dan perangkat lunak, tetapi juga mencakup perlindungan data serta kebijakan dan prosedur penggunaan sistem.

Dalam konteks platform e-commerce, keamanan sistem komputer memiliki peran yang sangat penting karena sistem tersebut mengelola data pengguna dalam jumlah besar, termasuk data pribadi dan informasi transaksi. Penerapan mekanisme keamanan seperti enkripsi, autentikasi, kontrol akses, fungsi hash, Message Authentication Code (MAC), dan digital signature menjadi kebutuhan utama untuk mencegah terjadinya kebocoran data dan penyalahgunaan informasi.

Menurut Stallings, keamanan sistem komputer harus dirancang secara menyeluruh dan berlapis (defense in depth) agar mampu menghadapi berbagai jenis ancaman yang terus berkembang. Dengan penerapan keamanan sistem komputer yang baik, kepercayaan pengguna terhadap suatu sistem dapat terjaga dan risiko kerugian akibat serangan siber dapat diminimalkan.

Keamanan Data Pengguna

Keamanan data pengguna merupakan upaya untuk melindungi data pribadi yang dimiliki oleh pengguna dari akses, penggunaan, pengungkapan, maupun perusakan oleh pihak yang tidak berwenang. Data pengguna pada sistem komputer, khususnya pada platform e-commerce, mencakup informasi sensitif seperti nama, alamat email, nomor telepon, kredensial akun, serta data transaksi. Perlindungan terhadap data tersebut menjadi aspek krusial karena berkaitan langsung dengan privasi dan kepercayaan pengguna.

Dalam sistem e-commerce, keamanan data pengguna harus diterapkan sejak proses pengumpulan, penyimpanan, hingga pengolahan data. Mekanisme keamanan yang umum digunakan meliputi enkripsi data, fungsi hash untuk penyimpanan kata sandi, kontrol akses, serta autentikasi pengguna. Tanpa penerapan keamanan yang memadai, data pengguna rentan terhadap berbagai ancaman seperti pencurian identitas, penyalahgunaan akun, dan kebocoran informasi pribadi.

Keamanan data pengguna juga berkaitan erat dengan prinsip Confidentiality, Integrity, dan Availability (CIA Triad). Kerahasiaan data menjamin bahwa informasi pengguna hanya dapat diakses oleh pihak yang berwenang, integritas data memastikan bahwa data tidak mengalami perubahan tanpa izin, dan ketersediaan data menjamin bahwa sistem dapat diakses ketika dibutuhkan oleh pengguna yang sah.

Kasus kebocoran data pada platform e-commerce, seperti kebocoran data Tokopedia tahun 2020, menunjukkan bahwa lemahnya perlindungan terhadap data pengguna dapat menimbulkan dampak yang signifikan, baik bagi pengguna maupun penyedia layanan. Oleh karena itu, penerapan keamanan data pengguna yang komprehensif dan berlapis sangat diperlukan untuk mencegah terjadinya insiden keamanan serupa di masa mendatang.

Fungsi Hash

Fungsi hash merupakan algoritma kriptografi yang digunakan untuk mengubah data dengan panjang variabel menjadi nilai hash dengan panjang tetap. Nilai hash ini bersifat unik untuk setiap input, sehingga perubahan kecil pada data masukan akan menghasilkan nilai hash yang berbeda secara signifikan. Fungsi hash bersifat satu arah (one-way function), yaitu nilai hash tidak dapat dikembalikan ke bentuk data asli.

Dalam keamanan sistem komputer, fungsi hash memiliki peran penting terutama dalam menjaga kerahasiaan dan integritas data. Pada platform e-commerce, fungsi hash umumnya digunakan untuk menyimpan kata sandi pengguna agar data asli tidak tersimpan secara langsung di dalam basis data. Dengan demikian, meskipun terjadi kebocoran data, kata sandi pengguna tetap tidak dapat diketahui secara langsung.

Fungsi hash yang baik memiliki beberapa karakteristik utama, yaitu:

1. Pre-image resistance, yaitu sulit untuk menemukan data asli dari nilai hash.
2. Second pre-image resistance, yaitu sulit menemukan input lain yang menghasilkan hash yang sama.
3. Collision resistance, yaitu kecil kemungkinan dua input berbeda menghasilkan nilai hash yang sama.

Algoritma hash yang umum digunakan dalam sistem keamanan antara lain SHA-256, SHA-512, dan bcrypt. Namun, penggunaan fungsi hash tanpa mekanisme tambahan seperti salt dapat meningkatkan risiko serangan brute force dan rainbow table. Oleh karena itu, praktik terbaik dalam penyimpanan kata sandi adalah mengombinasikan fungsi hash dengan salt dan iterasi yang cukup.

Dalam kasus kebocoran data Tokopedia tahun 2020, kata sandi pengguna dilaporkan tersimpan dalam bentuk hash. Meskipun hal ini menunjukkan adanya penerapan fungsi hash, risiko keamanan tetap ada apabila algoritma hash yang digunakan tidak disertai dengan perlindungan tambahan yang memadai.

Message Authentication Code (MAC)

Message Authentication Code (MAC) merupakan mekanisme kriptografi yang digunakan untuk menjamin integritas dan keaslian (autentikasi) suatu pesan atau data yang dikirimkan melalui sistem komputer. MAC bekerja

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

dengan menghasilkan sebuah kode autentikasi berdasarkan pesan dan sebuah kunci rahasia (secret key) yang hanya diketahui oleh pihak pengirim dan penerima.

Dalam prosesnya, pengirim menghasilkan nilai MAC dengan menggunakan algoritma tertentu, kemudian nilai tersebut dikirimkan bersama pesan. Penerima akan menghitung ulang nilai MAC menggunakan kunci rahasia yang sama dan membandingkannya dengan nilai MAC yang diterima. Jika kedua nilai tersebut sama, maka pesan dianggap asli dan tidak mengalami perubahan selama proses pengiriman.

MAC memiliki peran penting dalam keamanan sistem komputer, khususnya dalam menjaga integritas data dan mencegah manipulasi informasi oleh pihak yang tidak berwenang. Berbeda dengan fungsi hash yang tidak menggunakan kunci, MAC menggunakan kunci rahasia sehingga memberikan tingkat keamanan yang lebih tinggi terhadap serangan pemalsuan data.

Beberapa algoritma MAC yang umum digunakan antara lain HMAC (Hash-based Message Authentication Code), CMAC, dan GMAC. Dalam sistem e-commerce, MAC dapat digunakan untuk memastikan bahwa data transaksi, data pengguna, maupun komunikasi antara klien dan server tidak mengalami perubahan selama proses transmisi.

Penerapan MAC dalam sistem e-commerce sangat penting untuk mencegah serangan seperti man-in-the-middle dan modifikasi data. Namun, efektivitas MAC sangat bergantung pada keamanan pengelolaan kunci rahasia yang digunakan. Oleh karena itu, pengamanan kunci kriptografi menjadi faktor penting dalam penerapan MAC.

Digital Signature

Digital signature merupakan mekanisme kriptografi yang digunakan untuk menjamin keaslian (authentication), integritas (integrity), dan penyangkalan tidak dapat dilakukan (non-repudiation) terhadap suatu data atau pesan elektronik. Digital signature bekerja dengan memanfaatkan pasangan kunci kriptografi, yaitu kunci privat dan kunci publik, yang saling berhubungan secara matematis.

Pada proses pembuatannya, pengirim menghasilkan nilai hash dari pesan yang akan dikirim, kemudian nilai hash tersebut dienkripsi menggunakan kunci privat pengirim untuk membentuk digital signature. Penerima pesan akan melakukan verifikasi dengan mendekripsi digital signature menggunakan kunci publik pengirim dan membandingkannya dengan nilai hash pesan yang diterima. Apabila kedua nilai tersebut sama, maka pesan dapat dipastikan berasal dari pengirim yang sah dan tidak mengalami perubahan.

Digital signature memiliki peran penting dalam keamanan sistem komputer, terutama pada sistem e-commerce dan transaksi elektronik. Dengan adanya digital signature, sistem dapat memastikan bahwa transaksi yang dilakukan benar-benar berasal dari pihak yang berwenang serta mencegah terjadinya pemalsuan data dan penyangkalan transaksi.

Dalam platform e-commerce, digital signature digunakan untuk mengamankan transaksi pembayaran, validasi dokumen elektronik, serta autentikasi komunikasi antara server dan pihak ketiga. Penerapan digital signature yang baik dapat meningkatkan tingkat kepercayaan pengguna terhadap sistem dan meminimalkan risiko keamanan.

Namun, efektivitas digital signature sangat bergantung pada pengelolaan kunci kriptografi dan infrastruktur pendukung seperti Public Key Infrastructure (PKI). Tanpa pengelolaan kunci yang aman, digital signature dapat menjadi rentan terhadap penyalahgunaan.

Kebocoran Data (Data Breach)

Kebocoran data (*data breach*) merupakan insiden keamanan di mana data sensitif, rahasia, atau terlindungi diakses, dicuri, atau diungkapkan oleh pihak yang tidak berwenang. Data yang terdampak dalam kebocoran data umumnya meliputi data pribadi pengguna, informasi akun, serta data penting lainnya yang disimpan dalam suatu sistem komputer. Kebocoran data dapat terjadi akibat kelemahan sistem keamanan, kesalahan konfigurasi, maupun serangan siber yang disengaja.

Dalam konteks keamanan sistem komputer, kebocoran data sering kali disebabkan oleh berbagai faktor, seperti serangan peretas (*hacking*), malware, kerentanan aplikasi, serta lemahnya mekanisme autentikasi dan kontrol akses. Selain itu, faktor manusia (*human error*) juga menjadi salah satu penyebab utama terjadinya kebocoran data, misalnya penggunaan kata sandi yang lemah atau kelalaian dalam pengelolaan sistem.

Kebocoran data dapat menimbulkan dampak yang signifikan, baik bagi pengguna maupun penyedia layanan. Bagi pengguna, kebocoran data berpotensi menyebabkan pencurian identitas, penyalahgunaan akun, serta kerugian finansial. Sementara itu, bagi penyedia layanan e-commerce, kebocoran data dapat menurunkan tingkat kepercayaan pengguna, merusak reputasi perusahaan, serta menimbulkan konsekuensi hukum.

Kasus kebocoran data Tokopedia tahun 2020 merupakan contoh nyata insiden data breach pada platform e-commerce, di mana jutaan data pengguna dilaporkan bocor dan diperjualbelikan oleh pihak yang tidak bertanggung jawab. Peristiwa tersebut menunjukkan pentingnya penerapan keamanan sistem komputer yang kuat dan berlapis untuk melindungi data pengguna dari ancaman keamanan.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Oleh karena itu, pencegahan kebocoran data memerlukan penerapan berbagai mekanisme keamanan, seperti enkripsi data, fungsi hash untuk penyimpanan kata sandi, Message Authentication Code (MAC) untuk menjaga intergritas data, digital signature untuk autentikasi transaksi, serta audit keamanan system secara berkala.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi kasus (case study). Pendekatan kualitatif dipilih karena penelitian bertujuan untuk menganalisis secara mendalam permasalahan keamanan data pengguna pada platform e-commerce berdasarkan kejadian nyata, yaitu kebocoran data Tokopedia tahun 2020, tanpa melakukan pengujian sistem secara langsung.

Metode studi kasus digunakan untuk memahami fenomena kebocoran data secara kontekstual, meliputi kronologi kejadian, jenis data yang bocor, penyebab terjadinya kebocoran, serta solusi keamanan yang dapat diterapkan berdasarkan teori keamanan sistem komputer.

Objek dan Subjek Penelitian

Objek penelitian dalam jurnal ini adalah keamanan data pengguna pada platform e-commerce, dengan fokus pada sistem pengelolaan data pengguna.

Adapun subjek penelitian adalah kasus kebocoran data Tokopedia tahun 2020, yang melibatkan jutaan akun pengguna dan menjadi salah satu insiden keamanan siber terbesar di Indonesia.

Sumber Data Penelitian

Data yang digunakan dalam penelitian ini merupakan data sekunder, yang diperoleh dari berbagai sumber terpercaya, antara lain:

- Artikel berita nasional dan internasional terkait kebocoran data Tokopedia (Antara News, Kompas, The Jakarta Post).
- Jurnal ilmiah yang membahas keamanan sistem komputer, kriptografi, dan keamanan e-commerce.
- Buku referensi mengenai kriptografi dan keamanan jaringan.
- Dokumen dan publikasi yang membahas konsep hash function, Message Authentication Code (MAC), dan digital signature.

Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah:

- Studi Literatur, yaitu pengumpulan data melalui jurnal ilmiah, buku, dan publikasi akademik yang relevan dengan keamanan sistem komputer.
- Analisis Dokumen, yaitu pengkajian laporan berita dan artikel resmi terkait kebocoran data Tokopedia tahun 2020 untuk memperoleh informasi kronologi dan dampak kejadian.

Teknik Analisis Data

Analisis data dilakukan menggunakan beberapa teknik berikut:

- **Analisis Deskriptif**
  Digunakan untuk menjelaskan kronologi kebocoran data Tokopedia 2020, jenis data yang bocor, serta dampak yang ditimbulkan bagi pengguna dan perusahaan.
- **Analisis Keamanan Sistem Komputer**
  Analisis dilakukan berdasarkan prinsip Confidentiality, Integrity, dan Availability (CIA Triad) untuk mengevaluasi tingkat keamanan data pengguna.
- **Analisis Kriptografi**
  Digunakan untuk menilai penerapan:
  1. Hash Function dalam penyimpanan kata sandi pengguna,
  2. Message Authentication Code (MAC) dalam menjaga integritas data,
  3. Digital Signature dalam proses autentikasi dan validasi transaksi elektronik.
- **Analisis Perbandingan (Comparative Analysis)**
  Membandingkan praktik keamanan data yang diterapkan pada kasus Tokopedia dengan standar keamanan yang direkomendasikan dalam literatur dan best practice keamanan sistem komputer.
- **Analisis Solusi dan Rekomendasi**
  Digunakan untuk merumuskan solusi keamanan yang dapat diterapkan guna mencegah terjadinya kebocoran data serupa di masa mendatang.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Alur Penelitian

Tahapan penelitian yang dilakukan dalam jurnal ini meliputi:

1. Identifikasi permasalahan kebocoran data pada platform e-commerce.
2. Pengumpulan data melalui studi literatur dan analisis dokumen.
3. Analisis kasus kebocoran data Tokopedia 2020 berdasarkan prinsip keamanan sistem komputer.
4. Evaluasi penerapan hash, MAC, dan digital signature.
5. Penyusunan solusi dan rekomendasi keamanan data pengguna.

Keterbatasan Penelitian

Penelitian ini memiliki keterbatasan, yaitu tidak melakukan pengujian langsung terhadap sistem Tokopedia karena keterbatasan akses. Analisis dilakukan berdasarkan data sekunder dan referensi yang tersedia, sehingga hasil penelitian bersifat konseptual dan analitis.

HASIL DAN PEMBAHASAN

Gambaran Umum Kasus Kebocoran Data Tokopedia Tahun 2020

Berdasarkan hasil analisis terhadap data sekunder dan studi literatur, kebocoran data Tokopedia pada tahun 2020 merupakan salah satu insiden keamanan siber terbesar dalam sejarah *e-commerce* di Indonesia. Insiden ini melibatkan sekitar 91 juta akun pengguna, dengan data yang bocor mencakup nama pengguna, alamat email, nomor telepon, serta kata sandi yang tersimpan dalam bentuk *hash*. Data tersebut dilaporkan diperjualbelikan pada forum daring ilegal, sehingga meningkatkan risiko penyalahgunaan data pribadi pengguna (Kompas, 2020).

Kebocoran data ini menunjukkan bahwa platform *e-commerce* dengan basis pengguna yang besar menjadi target utama serangan siber. Nilai ekonomis data pribadi yang tinggi menjadikan perlindungan data sebagai aspek krusial dalam penyelenggaraan sistem perdagangan elektronik.

Analisis Keamanan Berdasarkan Prinsip CIA Triad

- **Confidentiality (Kerahasiaan)**
  Dari aspek *confidentiality*, insiden kebocoran data Tokopedia menunjukkan adanya kegagalan dalam menjaga kerahasiaan data pengguna. Data pribadi yang seharusnya dilindungi dan hanya dapat diakses oleh pihak berwenang justru berhasil diakses oleh pihak tidak bertanggung jawab. Hal ini mengindikasikan adanya kelemahan pada mekanisme kontrol akses atau perlindungan basis data. Menurut Stallings (2018), kerahasiaan data hanya dapat terjamin apabila sistem menerapkan autentikasi yang kuat, manajemen akses yang ketat, serta pendekatan keamanan berlapis (*defense in depth*). Meskipun Tokopedia telah menerapkan penyimpanan kata sandi dalam bentuk *hash*, kebocoran data dalam skala besar tetap menimbulkan risiko serius terhadap privasi pengguna, seperti serangan *phishing* dan *credential stuffing*.
- **Integrity (Integritas)**
  Berdasarkan laporan yang tersedia secara publik, tidak ditemukan indikasi adanya perubahan atau manipulasi data pengguna akibat insiden kebocoran tersebut. Namun, potensi pelanggaran integritas data tetap ada apabila penyerang memiliki kemampuan untuk memodifikasi data dalam sistem. Integritas data dapat dijaga melalui penerapan mekanisme kriptografi seperti *Message Authentication Code (*MAC*)* yang memastikan bahwa data tidak mengalami perubahan selama proses penyimpanan maupun transmisi (Menezes et al., 2018). Ketiadaan informasi mengenai penerapan *MAC* secara spesifik dalam sistem Tokopedia menunjukkan bahwa aspek integritas data masih memerlukan evaluasi dan penguatan lebih lanjut.
- **Availability (Ketersediaan)**
  Dari sisi *availability*, layanan Tokopedia tetap dapat diakses oleh pengguna setelah terjadinya insiden kebocoran data. Hal ini menunjukkan bahwa dampak utama insiden lebih berfokus pada pelanggaran kerahasiaan dibandingkan gangguan ketersediaan layanan. Namun demikian, menurut NIST (2020), insiden keamanan dalam skala besar berpotensi mengganggu operasional sistem apabila tidak ditangani dengan cepat. Oleh karena itu, ketersediaan layanan harus tetap menjadi perhatian utama dalam perancangan sistem keamanan *e-commerce*.

Evaluasi Penerapan Fungsi Hash dalam Perlindungan Kata Sandi

Hasil kajian menunjukkan bahwa Tokopedia telah menerapkan fungsi hash dalam penyimpanan kata sandi pengguna. Praktik ini sesuai dengan standar keamanan sistem komputer yang melarang penyimpanan kata sandi dalam bentuk *plaintext*. Namun, literatur keamanan menyatakan bahwa penggunaan fungsi *hash* saja belum cukup tanpa dikombinasikan dengan mekanisme tambahan seperti *salt* dan iterasi yang memadai (Stallings, 2018).

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Tanpa salt yang kuat, nilai hash kata sandi tetap berisiko untuk dipecahkan menggunakan serangan *brute force* atau *rainbow table*. Oleh karena itu, insiden kebocoran data Tokopedia menunjukkan bahwa implementasi kriptografi harus mengikuti praktik terbaik (*best practice*) secara menyeluruh untuk meminimalkan risiko kebocoran data sensitif.

Peran Message Authentication Code (MAC) dalam Menjaga Integritas Data

*Message Authentication Code (*MAC*)* berperan penting dalam menjamin integritas dan keaslian data. MAC bekerja dengan memanfaatkan kunci rahasia untuk memastikan bahwa data tidak dimodifikasi oleh pihak yang tidak berwenang. Algoritma MAC seperti HMAC-SHA256 direkomendasikan untuk melindungi data transaksi dan komunikasi antara klien dan server (Menezes et al., 2018).

Dalam konteks kasus Tokopedia, tidak terdapat informasi publik yang menjelaskan penerapan MAC secara rinci. Hal ini menunjukkan pentingnya audit keamanan internal dan transparansi penerapan mekanisme keamanan guna meningkatkan kepercayaan pengguna terhadap platform *e-commerce*.

Digital Signature dan Keamanan Transaksi Elektronik

Digital signature merupakan mekanisme kriptografi yang digunakan untuk menjamin keaslian, integritas, dan *non-repudiation* dalam transaksi elektronik. Dalam sistem *e-commerce*, digital signature berperan penting dalam mengamankan transaksi pembayaran dan komunikasi antar sistem.

Meskipun digital signature tidak secara langsung mencegah kebocoran data pengguna, penerapannya dapat meningkatkan keamanan sistem secara keseluruhan. Menurut Menezes et al. (2018), penggunaan *digital signature* berbasis *Public Key Infrastructure (*PKI*)* dapat mengurangi risiko pemalsuan data dan meningkatkan kepercayaan pengguna terhadap sistem elektronik.

Implikasi Tata Kelola dan Regulasi Perlindungan Data

Kebocoran data Tokopedia juga memiliki implikasi signifikan terhadap tata kelola dan regulasi perlindungan data di Indonesia. Insiden ini mempertegas pentingnya penerapan kebijakan perlindungan data pribadi yang komprehensif serta tanggung jawab penyedia layanan digital dalam menjaga keamanan data pengguna.

Penerapan Undang-Undang Perlindungan Data Pribadi (UU PDP) menegaskan bahwa penyedia layanan *e-commerce* memiliki kewajiban hukum untuk melindungi data pribadi dan melaporkan insiden kebocoran data. Dengan demikian, keamanan data tidak hanya menjadi isu teknis, tetapi juga bagian dari tanggung jawab hukum dan etika perusahaan.

KESIMPULAN

Berdasarkan analisis yang dilakukan terhadap kasus kebocoran data Tokopedia tahun 2020, dapat disimpulkan bahwa insiden keamanan pada platform *e-commerce* tidak hanya disebabkan oleh satu faktor tunggal, melainkan kombinasi dari kerentanan teknis dan manajemen keamanan. Meskipun Tokopedia telah menerapkan mekanisme kriptografi berupa fungsi *hash* untuk melindungi kata sandi pengguna, insiden ini membuktikan bahwa perlindungan data harus bersifat menyeluruh (*defense in depth*). Kegagalan dalam menjaga kerahasiaan (*confidentiality*) data pengguna menunjukkan adanya celah pada kontrol akses sistem, yang memungkinkan pihak tidak berwenang mengekstraksi informasi sensitif dalam jumlah besar.

Penelitian ini juga menegaskan peran krusial dari penerapan standar kriptografi yang ketat. Penggunaan fungsi *hash* harus selalu disertai dengan mekanisme *salt* yang kuat untuk mencegah serangan *brute force* atau *rainbow table*. Selain itu, implementasi *Message Authentication Code* (MAC) dan *Digital Signature* sangat vital untuk menjamin integritas (*integrity*) dan keaslian data selama proses transmisi dan transaksi, guna mencegah manipulasi data serta penyangkalan transaksi (*non-repudiation*) di kemudian hari.

Sebagai rekomendasi, penyedia layanan *e-commerce* perlu melakukan audit keamanan secara berkala dan memperkuat arsitektur keamanan mereka, tidak hanya pada penyimpanan data tetapi juga pada jalur distribusi data. Bagi pengguna, penerapan otentikasi dua faktor (2FA) dan penggantian kata sandi secara berkala menjadi langkah mitigasi mandiri yang wajib dilakukan.

Keterbatasan penelitian ini terletak pada penggunaan data sekunder tanpa pengujian penetrasi langsung terhadap sistem terkait. Oleh karena itu, penelitian selanjutnya disarankan untuk mengeksplorasi analisis teknis yang lebih mendalam atau simulasi serangan pada lingkungan *sandbox* untuk menguji efektivitas algoritma keamanan terbaru dalam mencegah insiden serupa.

UCAPAN TERIMA KASIH

Penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada bapak T. Sukma Achriadi Sukiman, S.Kom., M.Kom selaku dosen pengampu mata kuliah Keamanan Sistem Komputer (A3) yang telah memberikan arahan

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

dan bimbingan selama proses penulisan jurnal ini. Terima kasih juga kepada rekan-rekan mahasiswa Universitas Malikussaleh yang telah berdiskusi dan berbagi referensi.

REFERENSI

(NIST), N. I. of S. and T. (2020). *Computer Security Incident Handling Guide*.

Brown, W. S. L. (2018). *Computer Security: Principles and Practice (4th Edition)*. Pearson.

Burhan, F. A. (2021). *Tokopedia Ungkap Cara Atasi Kasus Kebocoran Data Pribadi*. KataData.

Kompas.com. (2020). *Fakta di Balik Bobolnya 91 Juta Data Pengguna Tokopedia*. https://tekno.kompas.com/read/2020/05/03/10230027/fakta-di-balik-bobolnya-91-juta-data-pengguna-tokopedia

News, A. (2020). *Pakar keamanan siber ungkap kronologi kebocoran data Tokopedia*. https://www.antaranews.com/berita/1463133/pakar-keamanan-siber-ungkap-kronologi-kebocoran-data-tokopedia

Pfleeger, C. P., Pfleeger, S. L., & John, M. (2015). Security in Computing, Fifth Edition. *Computers & Security*, *16*(5), 181. https://testbankati.com/wp-content/uploads/2020/10/9780134085043_SolutionManual_ch1.pdf

Stallings, W. (2017). Cryptography and Network Security: Principles and Practices. In *Cryptography and Network Security* (4th ed.). Prentice Hall. http://www.amazon.com/Cryptography-Network-Security-William-Stallings/dp/0131873164

Standardization., I. O. for. (2022). *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements.*

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (2022).

Vanstone, A. J. M. P. C. van O. S. A. (2018). *Handbook of Applied Cryptography*. CRC Press.