MADINAVERSE: Jurnal Informatika, IoT dan Games
Vol. 1, No. 1, Desember 2024

Keamanan Data dalam Penggunaan IoT untuk Menghimpun dan Mengelola Big Data

Syahla Nadya Putri Syabrina
Program Studi Teknik Informatika, Fakultas Ilmu Rekayasa, Universitas Paramadina
Email: syahla.putri@students.paramadina.ac

Abstrak - Dalam era pertumbuhan sistem informasi yang pesat, pemanfaatan Internet of Things (IoT) dan Big Data telah menjadi fokus utama perusahaan modern. Perangkat IoT, yang terhubung ke internet, memainkan peran penting dalam mengumpulkan, mentransmisikan, dan mengolah data dari berbagai sumber. Sementara itu, Big Data adalah istilah yang menggambarkan jumlah data yang besar dan beragam, jika dimanfaatkan dengan baik, dapat memberikan berbagai keuntungan. Namun, dengan meningkatnya penggunaan IoT dan Big Data, perlindungan keamanan informasi menjadi semakin penting. Tujuan dari penelitian ini adalah untuk menganalisis tantangan utama dalam keamanan data terkait penggunaan IoT untuk mengelola Big Data. Metode penelitian menggunakan kajian literatur dari berbagai artikel jurnal nasional dan internasional yang relevan. Hasil analisis menunjukkan bahwa tantangan utama meliputi pengumpulan data yang luas, keamanan data, identifikasi individu, kontrol pengguna, dan akses data oleh pihak ketiga. Oleh karena itu, integrasi yang seimbang antara teknologi IoT, Big Data, dan praktik keamanan data menjadi kunci untuk memastikan keberhasilan dan keberlanjutan bisnis di era digital ini.

Kata kunci: Keamanan Data, IoT, Big Data, Pengumpulan Data, Perlindungan Informasi

Abstrak - In the era of rapid information system growth, the utilization of the Internet of Things (IoT) and Big Data has become a primary focus for modern companies. IoT devices, which are connected to the internet, play a crucial role in collecting, transmitting, and processing data from various sources. Meanwhile, Big Data describes large and diverse datasets that, if properly leveraged, can provide numerous benefits. However, with the increasing use of IoT and Big Data, the protection of information security becomes increasingly important. The aim of this study is to analyze the main challenges in data security related to the use of IoT for managing Big Data. The research method involves a literature review of various relevant national and international journal articles. The results indicate that the main challenges include extensive data collection, data security, individual identification, user control, and third-party data access. Therefore, a balanced integration of IoT technology, Big Data, and data security practices is key to ensuring business success and sustainability in this digital era.

Keywords: Data Security, IoT, Big Data, Data Collection, Information Protection

I. PENDAHULUAN

Di era perkembangan pesat sistem informasi, penggunaan Internet of Things (IoT) dan big data telah menjadi perhatian utama bagi perusahaan-perusahaan modern.Perangkat IoT, yang merupakan perangkat fisik terhubung ke internet, memainkan peran penting dalam mengumpulkan, mentransmisikan, dan mengolah data dari berbagai sumber, termasuk sensor, transaksi, dan aktivitas digital lainnya. Di sisi lain operasional, inovasi produk dan layanan, strategi pemasaran yang efektif, serta deteksi penipuan dan keamanan.

Namun, dengan meningkatnya penggunaan IoT dan big data, perlindungan keamanan informasi menjadi semakin penting. Informasi yang tidak dilindungi
dengan baik dapat jatuh ke tangan yang tidak bertanggung jawab, menyebabkan ketidakakuratan data dan bahkan bisa menjadi sumber informasi yang menyesatkan. Oleh karena itu, system keamanan data harus mampu mengidentifikasi, mengotentifikasi, dan memberikan izin dengan tepat kepada pengguna. Berbagai serangan atau peretasan, seperti gangguan sistem, penolakan layanan, vandalisme dan lainnya, dapat mengancam integritas data dan keamanan sistem [1].

Tujuan dari keamanan data dalam penggunaan IoT untuk menghimpun dan mengelola big data adalah untuk melindungi sistem dari berbagai ancaman dan untuk mendeteksi serta memperbaiki kerusakan yang mungkin terjadi. Pendekatan yang efektif dalam mengelola data dan komunikasi antar objek IoT harus mencakup penggunaan algoritma pemograman yang tepat, yang tidak harus mengoptimalkan kinerja sistem tetapi juga menjaga keamanan data yang dikirim dan diterima. Dengan demikian, integrasi yang seimbang antara penggunaan IoT, Big data, dan keamanan data menjadi kunci dalam memastikan keberhasilan dan keberlanjutan bisnis modern di era digital ini [2].

Dalam konteks tersebut, tujuan dari penelitian ini adalah untuk menganalisis dan memahami tantangan utama yang

dihadapi dalam menjaga keamanan data pada penggunaan IoT untuk mengelola big data.

II. METODE PENELITIAN

Penulis menggunakan kajian literatur dengan mencari berbagai artikel dari jurnal nasional dan internasional melalui Google Scholar yang relevan dengan topik yang dibahas. Langkah-langkah dalam menggunakan kajian literatur ini mencakup pemilihan topik, pengumpulan sumber literatur yang mendukung topik tersebut, pengkajian literatur yang relevan untuk menyusun pembahasan tentang kemampuan berpikir kreatif matematis, serta menyimpulkan dan memberikan saran berdasarkan hasil dari kajian [3].

III. ANALISIS DATA

Dalam revolusi industri, interkoneksi antara IoT dan Big Data memiliki dampak yang signifikan dalam upaya meningkatkan efisiensi operasional perusahaan. Gabungan teknologi ini memungkinkan penggunaan data yang dikumpulkan dari berbagai sumber, seperti sensor, perangkat mobile, media sosial, dan transaksi bisnis, untuk mengoptimalkan proses operasional. Melalui IoT, perusahaan dapat memantau dan mengendalikan proses produksi secara real time, sementara Big Data digunakan untuk menganalisis data tersebut guna mengidentifikasi potensi peningkatan efisiensi produk serta untuk menyempurnakan jadwal produksi. Pemanfaatan Big Data dan IoT membawa manfaat signifikan dalam meningkatkan efisiensi, mengurangi biaya operasional dan meningkatkan kualitas produk yang dihasilkan [4].

Di era digital yang semakin berkembang, berbagai aktivitas juga semakin meluas jangkauannya, maka itu akan memberikan ancaman baru terhadap keamanan data diri, data perusahaan dan potensi pelanggaran privasi. Diperlukannya pemahaman yang lebih mendalam mengenai praktik aman dalam penggunaan teknologi digital Keamanan data mengacu pada tindakan perlindungan yang diambil untuk mengamankan data dari akses yang tidak disetujui dan untuk menjaga kerahasiaan, integritas dan ketersediaan data. Praktik perlindungan data yang efektif mencakup teknik perlindungan data seperti enkripsi data, manajemen kunci, redaksi data, subsetting data dan penyembunyiaan data, serta control akses khusus dan hak pemantauan [5].

A. Keamanan Pengguna IoT dalam mengelola Big Data

Penggunaan Internet of Things (IoT) untuk mengumpulkan dan mengelola Big Data semakin umum digunakan di berbagai sektor industri seperti kesehatan, manufaktur, transportasi, energi, dan lainnya. IoT memfasilitasi koneksi perangkat dan sensor ke internet, menghasilkan data besar dan beragam yang kemudian dianalisis menggunakan teknologi Big Data. Keamanan dalam IoT adalah praktik yang menjaga sistem IoT agar aman, melindungi dari ancaman dan pelanggaran, serta mengidentifikasi dan mengurangi risiko. Hal ini penting untuk memastikan ketersediaan, kerahasiaan, dan integritas solusi IoT. Perhatian terhadap keamanan privasi dalam IoT juga penting karena harus diintegrasikan dengan baik.

Berikut ini adalah konsep-konsep keamanan yang penting dalam Internet of Things (IoT) yang perlu dipahami:

1. Identifikasi dan otentikasi di mana setiap perangkat harus diidentifikasi dan diautentikasi sebelum diizinkan berinteraksi dengan perangkat lain.
2. Data yang dikirim harus dienkripsi untuk menjaga kerahasiaan, sementara jaringan IoT harus dilindungi dengan firewall dan deteksi intrusi.
3. Pengelolaan akses dan otorisasi penting untuk memastikan peran yang tepat bagi pengguna dan perangkat, sementara pemantauan keamanan dan pembaruan perangkat lunak secara teratur juga krusial.
4. Perlindungan fisik perangkat keras IoT dan pengujian keamanan yang komprehensif juga diperlukan untuk mengidentifikasi dan mengatasi potensi kerentanan.

Dengan menerapkan konsep-konsep ini, keamanan IoT dapat ditingkatkan secara signifikan [6].

IV. HASIL ANALISIS DATA

Keamanan dan kerahasiaan data merupakan perhatian utama dalam era big data yang semakin berkembang. Sebagian besar pemilik dan penyedia layanan big data saat ini seringkali tidak memiliki kapasitas untuk mengelola dan menganalisis volume data yang besar tersebut. Oleh karena itu, mereka cenderung mengirimkan data tersebut ke pihak ketiga untuk diproses, namun hal ini juga dapat menimbulkan potensi masalah keamanan data sensitif tersebut. Masalah keamanan dan privasi menjadi semakin penting seiring dengan kemajuan teknologi, terutama dalam bidang seperti perbankan dan telekomunikasi yang seringkali memiliki akses langsung terhadap data pribadi pelanggan mereka. Untuk melindungi data individu, pemerintah biasanya membentuk regulasi seperti Undang-Undang Perlindungan Data dan Informasi Pribadi serta regulasi lainnya yang mengatur penggunaan dan perlindungan data secara lebih tepat. Kendati demikian, tantangan privasi data juga muncul dari pemanfaatan teknologi big data yang kurang bijaksana, yang dapat mengancam stabilitas negara dan keamanan warga negara [7] [8]. Oleh karena itu, keamanan dalam pengelolaan big data harus diperhatikan secara serius.

Berikut tantangan yang perlu diperhatikan dalam menggunakan Internet of Things (IoT) untuk mengumpulkan dan mengelola Big Data :

1. Pengumpulan data yang luas, Setiap perangkat IoT dapat mengumpulkan data tentang aktivitas pengguna, preferensi, lokasi, dan lainnya. Tantangan privasi terkait dengan bagaimana data ini dikumpulkan, digunakan, dan disimpan dengan aman.

2. Keamanan Data: Karena perangkat IoT terhubung ke internet, mereka rentan terhadap serangan siber. Jika tidak ada langkah-langkah keamanan yang memadai, data pribadi yang dikumpulkan oleh perangkat IoT bisa diakses oleh pihak yang tidak berwenang. Perlindungan data harus menjadi prioritas untuk menjaga privasi pengguna [9], [10].

3. Identifikasi Individu: Data yang dikumpulkan oleh perangkat IoT bisa mengungkap identitas individu secara langsung atau tidak langsung. Pola aktivitas sehari-hari atau informasi geografis yang dikumpulkan oleh perangkat pintar dapat mengidentifikasi kebiasaan dan rutinitas individu dengan mudah. Hal ini dapat mengancam privasi dan keamanan individu [11], [12].

4. Kontrol Pengguna: Penggunaan perangkat IoT bisa mengurangi kontrol pengguna atas data pribadi mereka. Pengguna harus dapat memahami dan mengendalikan penggunaan data mereka oleh perangkat IoT serta pihak lain dalam ekosistem IoT. Kejelasan dan transparansi dalam kebijakan privasi serta opsi untuk mengontrol pengumpulan dan penggunaan data sangat penting [13].

5. Akses Data oleh Pihak Ketiga, Data yang dikumpulkan oleh perangkat IoT dapat dibagikan dengan pihak ketiga seperti penyedia layanan atau mitra bisnis. Pembagian data ini meningkatkan risiko privasi. Diperlukan kebijakan dan persyaratan yang jelas tentang penggunaan dan pembagian data untuk menjaga privasi pengguna [14], [15].

V. KESIMPULAN

Dalam era pertumbuhan sistem informasi yang pesat, pemanfaatan Internet of Things (IoT) dan Big Data menjadi fokus utama perusahaan modern. Meskipun menawarkan manfaat yang besar, tantangan keamanan data menjadi perhatian utama dalam penggunaan IoT untuk menghimpun dan mengelola Big Data. Perlindungan data yang luas, keamanan data selama transit dan penyimpanan, identifikasi individu, kontrol pengguna, dan akses data oleh pihak ketiga adalah aspek-aspek yang perlu diperhatikan dengan serius. Integrasi yang seimbang antara teknologi IoT, Big Data, dan praktik keamanan data menjadi kunci untuk menghadapi risiko serangan siber, pelanggaran privasi, dan kerentanan sistem. Hasil analisis menjelaskan bahwa tantangan keamanan data yang terkait dengan penggunaan IoT untuk mengelola Big Data ialah pengumpulan data yang luas, keamanan data, identifikasi individu, kontrol pengguna, akses data oleh pihak ketiga. Oleh karena itu, upaya perlindungan data yang efektif melalui teknik-teknik keamanan seperti enkripsi, manajemen akses, dan pemantauan secara teratur menjadi sangat penting dalam memastikan keberhasilan dan keberlanjutan bisnis di era digital ini.

REFERENSI

[1] Eka Mayasari and Agussalim Agussalim, “Literature Review: Big Data dan Data Analys pada Perusahaan,” *J. Ilm. Sist. Inf. dan Ilmu Komput.*, vol. 3, no. 3, pp. 171–187, 2023, doi: 10.55606/juisik.v3i3.680.

[2] Edy Soesanto, Nova Astia Ningsih, Lili Khoerunisa, and Muhammad Ilham Faturrahman, “Keamanan Informasi Data Dalam Pemanfaatan Teknologi Informasi Pada PT Bank Central Asia (BCA),” *Student Res. J.*, vol. 1, no. 3, pp. 227–238, 2023, doi: 10.55606/srjyappi.v1i3.334.

[3] D. J. Sengkey, P. Deniyanti Sampoerno, and T. A. Aziz, “Kemampuan Pemahaman Konsep Matematis: Sebuah Kajian Literatur,” *Griya J. Math. Educ. Appl.*, vol. 3, no. 1, pp. 67–75, 2023, doi: 10.29303/griya.v3i1.265.

[4] S. A. Putri, Y. Nabela, M. Arifan, R. Hidayat, and M. Ikaningtyas, “Optimalisasi Proses Operasional dengan Menggabungkan Teknologi IoT dan Big Data : Studi Kasus pada PT Pertamina dalam Industri Minyak dan Gas Operational Process Optimization by Combining IoT and Big Data Technology : A Case Study on PT Pertamina in the O,” vol. 3, no. 1, pp. 1–10, 2024.

[5] S. Ceri, “Data-Centric Systems and Applications Series editors”.

[6] F. Prasetyo Eka Putra, S. Mellyana Dewi, and A. Hamzah, “Jurnal Sistim Informasi dan Teknologi https://jsisfotek.org/index.php Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari : Tantangan dan Implikasi,” vol. 5, no. 2, pp. 26–32, 2023, doi: 10.37034/jsisfotek.v5i1.232.

[7] N. S. Nainggolan and I. P. Nasution, “Pentingnya Keamanan Big Data Dalam Lembaga Pemerintahan Di Era Digital,” *J. Sains dan Teknol.*, vol. 3, no. 2, pp. 253–257, 2023, doi: 10.47233/jsit.v3i2.883.

[8] Y. Daeng, J. Levin, M. Razzaq Prayudha, N. Putri Ramadhani, S. Imanuel, and A. Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia Yusuf Daeng, “Analisis Penerapan Sistem Keamanan Siber TerhadapKejahatan Siber Di Indonesia,” *J. Soc. Sci. Res.*, vol. 3, no. 6, pp. 1135–1145, 2023.

[9] R. Rizal, N. Widiyasono, and S. Yuliyanti, “Kecerdasan Buatan untuk Klasifikasi Serangan Siber pada Internet of Things Network Traffic,” *Jumanji*, vol. 7, no. 2, pp. 2598–8069, 2023.

[10] R. Pratama Putra *et al.*, “Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi,” *Innov. J. Soc. Sci. Res.*, vol. 3, no. 6, pp. 2898–2905, 2023, [Online]. Available: https://j-innovative.org/index.php/Innovative/article/view/6662

[11] J. Manurung, A. P. E. Sihombing, and B. Pandiangan, “Sosialisasi Dan Edukasi Tentang Keamanan Data Dan Privasi Di Era Digital Untuk Meningkatkan Kesadaran Dan Perlindungan Masyarakat,” *J. Pengabdi. Masy. Nauli*, vol. 2, no. 1, pp. 1–7, 2023, [Online]. Available:

https://ejournal.marqchainstitute.or.id/index.php/Nauli/article/view/103

[12] Khoiri Gusnanda, Nur Ulfadillah, and Titin Sumarni, "Struktur Basis Data Di Era Digital (Implementasi Pengamanan Basis Data Di Era Global)," *J. Sains dan Teknol.*, vol. 3, no. 7, pp. 100–111, 2024, [Online]. Available: https://ejournal.warunayama.org/kohesi

[13] H. W. Saputra and I. Komputer, "Penerapan kecerdasan buatan dalam pengujian perangkat lunak," vol. 1, no. 2, pp. 1–16, 2024.

[14] D. Natalia and A. A. Sudiro, "Anak yang Menjadi Korban/Pelaku/Saksi; Pelindungan anak; Hak-Hak anak," vol. 5, no. 1, 2024.

[15] T. G. Laksana and S. Mulyani, "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan," *J. Ilm. Multidisiplin*, vol. 3, no. 01, pp. 109–122, 2024, doi: 10.56127/jukim.v3i01.1143.