e-ISSN:2829-4580, p-ISSN: 2829-4599
DOI: https://doi.org/10.38035/jim.v2i1
Received: 10 Mei 2023, Revised: 30 Mei 2023, Publish: 31 Mei 2023

GREENATION GLOBAL RESEARCH NATIONAL
JIM
JURNAL ILMU MULTIDISIPLIN
E-ISSN:2829-4580, P-ISSN=2829-4599
https://greenpub.org/JIM
editor@greenpub.org
0811 7401 455

Pentingnya Kemanan Data dalam Intelijen Bisnis

Rizky Febrian[1], Achmad Fauzi[2], Tegar Maulana Hidayat[3], Rifki Ardian[4], Alfito Surya Saputra[5]
[1.] Universitas Bhayangkara Jakarta Raya, Indonesia, rizkyfebrian352@gmail.com
[2.] Universitas Bhayangkara Jakarta Raya, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id
[3.] Universitas Bhayangkara Jakarta Raya, Indonesia, tegarmaulanahidayat28@gmail.com
[4.] Universitas Bhayangkara Jakarta Raya, Indonesia, Rifkiardian11355@gmail.com
[5.] Universitas Bhayangkara Jakarta Raya, Indonesia, alfitosurya18@gmail.com

Corresponding Author: Rizky Febrian

Abstract: *The main objective of this research is to evaluate the impact of implementing business intelligence tools on data security. Organizational data integrity is very important, as it is their most valuable asset. Organizations are expected to be able to enrich data from the use of internet-connected gadgets because their use is already widespread in all industries. When it comes to managing and protecting corporate data, data security issues rank first on the list of concerns. Data from the past and present is used to make guesses and predictions. Threats, data loss, and data manipulation are all ways in which a data security breach can harm an organization. Most BI systems rely on plug-ins connected to the internet. Without anti-malware and firewall protection, hackers can compromise the system browser and remove all of its plug-ins. Inadequate security measures on mobile devices make it easy for hackers to monitor system vulnerabilities and launch attacks through data manipulation or theft. The prospect of increasing investment through the creation of new markets can be realized with the right data security measures to ensure the smooth running of all business processes.*

Keyword: *Data Security, Business Intelligence, Business Systems, Internet of Things.*

Abstrak: Tujuan utama dari penelitian ini adalah untuk mengevaluasi dampak penerapan alat intelijen bisnis terhadap keamanan data. Integritas data organisasi sangat penting, karena merupakan aset mereka yang paling berharga. Organisasi diharapkan dapat memperkaya data dari penggunaan gadget yang terhubung dengan internet karena penggunaannya sudah meluas di semua industri. Dalam hal mengelola dan melindungi data perusahaan, masalah keamanan data menempati urutan pertama dalam daftar kekhawatiran. Data dari masa lalu dan sekarang digunakan untuk membuat tebakan dan prediksi. Ancaman, kehilangan data, dan manipulasi data adalah semua cara di mana pelanggaran keamanan data dapat membahayakan organisasi. Sebagian besar sistem BI mengandalkan plug-in yang terhubung ke internet. Tanpa

perlindungan anti-malware dan firewall, peretas dapat membahayakan browser sistem dan menghapus semua plug-innya. Langkah-langkah keamanan yang tidak memadai pada perangkat seluler memudahkan peretas untuk memantau kerentanan sistem dan meluncurkan serangan melalui manipulasi atau pencurian data. Prospek peningkatan investasi melalui penciptaan pasar baru dapat diwujudkan dengan langkah pengamanan data yang tepat untuk menjamin kelancaran seluruh proses bisnis.

Kata Kunci: Keamanan Data, Business Intelligence, Sistem Bisnis, Internet of Things.

PENDAHULUAN

Teknologi perusahaan yang sedang naik daun, intelijen bisnis mengambil pendekatan teknologi yang berorientasi pada proses untuk perencanaan dan pengambilan keputusan. Kecerdasan bisnis adalah alat yang membantu eksekutif dan manajer menganalisis data dan informasi untuk membuat pilihan bisnis yang lebih baik. Istilah "intelijen bisnis" mengacu pada proses di mana bisnis mengumpulkan informasi dan data yang berguna baik dari sumber internal maupun eksternal dengan menggunakan berbagai teknik dan instrument.

biasa dalam proses Intelijen bisnis, analitik membantu perencanaan jangka panjang dan jangka pendek. Ketersediaan luas konektivitas Internet telah memungkinkan bisnis untuk menyediakan staf mereka dengan perangkat yang berbeda yang semuanya dapat berbagi jaringan yang sama. Membawa perangkat IoT ke tempat kerja memiliki manfaat besar bagi manajemen perusahaan dan perencanaan strategis. IoT terlihat sangat berguna untuk memperkirakan dan menilai penjualan dan memahami strategi pasar, berkat manfaatnya dalam kecerdasan bisnis. Keefektifan model prediksi telah dipelajari sebelumnya untuk melihat apakah ada dampaknya. (Rozi, 2020). Kegiatan operasional bisnis dapat ditingkatkan dengan penerapan internet of things di industri bisnis.

Dalam hal intelijen bisnis, internet of things memiliki potensi untuk meningkatkan atau sangat menghambat kemampuan staf manajemen tingkat atas untuk memanfaatkan data yang lebih kaya dalam pengembangan rencana dan strategi perusahaan. Landasan intelijen bisnis adalah integrasi informasi baru dengan data yang ada untuk mengidentifikasi tren dan perkembangan.

IoT sangat cocok untuk menghitung dan memproyeksikan data masa depan untuk perusahaan komersial. Kecerdasan bisnis mendapat banyak manfaat dari meluasnya penggunaan data besar dan komputasi awan. Dengan penggunaan infrastruktur cloud computing, IoT dapat secara signifikan memengaruhi kecerdasan perusahaan melalui penerapan big data melalui proses identifikasi, analisis, dan penemuan data. Informasi yang digunakan oleh IoT berasal dari berbagai tempat, baik internal maupun eksternal.

Ada sejumlah masalah potensial yang mungkin muncul saat menggunakan platform IoT untuk informasi bisnis. Pada bagian ini, kita akan membicarakan beberapa masalah keamanan dan bahaya lain yang mungkin Anda hadapi. Di bagian selanjutnya, kami juga akan membahas pendekatan untuk mengatasi berbagai kesulitan, masalah, dan bahaya yang terkait dengan keamanan data. Pada bagian ini, kita akan melihat pro dan kontra dari intelijen bisnis. Pada bagian terakhir ini, kami akan menarik beberapa kesimpulan berdasarkan data yang ditawarkan sebelumnya.

METODE

Karya ilmiah ditulis dengan menggunakan pendekatan kualitatif dan penelitian kepustakaan yang ekstensif. Menganalisis teori dan hubungan/efek antar variabel di buku perpustakaan, jurnal online, dan sumber online lainnya seperti Mendeley, Scholar Google, dan lain-lain. Penggunaan literature review dalam penelitian kualitatif harus mengikuti

standar metodologi yang telah ditetapkan. Hal ini memerlukan pendekatan induktif, dimana data tidak boleh mempengaruhi pertanyaan yang akan dijawab. Studi eksplorasi sering dilakukan oleh peneliti kualitatif (Ali & Limakrisna, 2013).

Tabel 1: Penelitian terdahulu yang relavan

No	Author (tahun)	Hasil riset terdahulu	Persamaan	Perbedaan
1	Gihon lim, Sahrudin, Viorentika Damar Wengi dan Noviandi (2023)	Analisis data dan IoT akan berdampak positif pada bisnis, baik di berbagai sektor industri	Platform IoT berdampak positif pada inteligen bisnis	Pengaruh IoT berdampak positif pada layanan inteligen bisnis
2	Syifaul Fauda, Endah Setyowati, Dwi Wahyu Riani dan Galuh Inti Aulia (2023)	IoT telah berkembang sangat pesat di beragam sektor, dan salah satu dari sekian banyak corcern dan potensial adalah sektor pertanian	Berkembangnya peran IoT dari beberapa sektor	IoT telah berkembang pesat di sektor bisnis
3	Iswahyudhi Utari Turyadi, Firman Johan, dan Dadang Widyanto (2021)	IoT telah membawa pengaruh positif terhadap peningkatan kualitas inteligen	Adanya platform IoT telah meningkatkan efisiensi operasional organisasi	Penerapan platform IoT membantu melacak data waktu nyata dengan menyediakan akses yang jelas ke data historis.
4	Zen Munawar dan Novianti Indah Putri (2020)	Pada penelitian ini membuktikan bahwa efisiensi dan kelayakan menggunakan deep learning dan teknologi big data pada keamanan IoT	Perangkat IoT terbukti rentan karena baru-baru ini adanya peningkatan serangan seperti, Botna, Carna dan Mirai.	Menerapkan platform IoT membantu melacak data waktu nyata dengan menyediakan akses yang jelas ke data historis
5	Fahrur Rozi (2020)	Penggunaan IoT sangat berpengaruh positif dan efisien untuk perbaikan data dan prediksi dengan pembelajaran keputusan	Perkembangan teknologi dan informasi membawa perubahan besar di segala bidang khususnya Internet of Things(IoT). Dengan adanya IoT, sejumlah perangkat yang terhubung ke internet mulai dari sensor dan Ponsel pintar meningkat secara signifikan.	Penelitian ini membahas perspektif beberapa masalah dan solusi keamanan informasi pada platform Internet of Things, yang akan diikuti oleh penelitian selanjutnya.
6	I Nyoman Buda Hartawan dan I Wayan Sudiarsa (2019)	Sistem IoT dapat mengontrol untuk menyalakan/ mematikan lampu dari jarak jauh melalui internet menggunakan smartphone	Teknologi Internet of Things (IoT) memungkinkan untuk memantau dan mengontrol kondisi lingkungan	Teknologi Internet of Thing dapat digunakan untuk melacak data dengan menyediakan akses yang jelas.

			dan perangkat elektronik dari jarak jauh melalui internet.	

HASIL DAN PEMBAHASAN

Hasil Penelitian

Botnet Attacks

Menghubungkan banyak perangkat menjadi satu botnet. Serangan botnet dilakukan dengan tujuan mengganggu operasi reguler atau mengurangi kualitas layanan yang diberikan oleh sistem yang ditargetkan. (Internet et al., 2023). Untuk meluncurkan serangan seperti itu, Botnet yang tangguh harus dirakit terlebih dahulu. Gambar 1 menggambarkan langkah selanjutnya dalam siklus serangan, saat botnet6 dilepaskan ke jaringan dan mulai menyerang beberapa komputer secara bersamaan. Permintaan serangan intelijen bisnis di internet sering kali berbentuk pesan teks atau email. Kecerdasan bisnis dapat terhambat oleh serangan semacam ini karena untuk sementara membekukan server dan karenanya memperlambat seluruh jaringan.(F. Bromberg, D. Dujovne, T. Watteyne, A. L. Diedrichs, 2018).

Denial of Service

Kecerdasan bisnis pada platform IoT menghadapi tantangan seperti penolakan serangan layanan. Penolakan layanan terjadi ketika layanan tidak tersedia selama proses yang terjadi secara normal. (Nohuz et al., 2014). Ada sejumlah potensi penyebab gangguan layanan. Pengenalan file berbahaya dalam sistem organisasi dapat memengaruhi sejumlah besar komputer yang digunakan untuk intelijen bisnis dalam kerangka serangan denial of service terdistribusi. (D. Goel, S. Chaudhury, 2017). Jika penyerang menyuntikkan kode file berbahaya ke dalam sistem organisasi, itu akan berdampak negatif di mana data tidak dapat diakses oleh karyawan atau bisnis itu sendiri, mencegahnya membuat keputusan strategis yang tepat.

Saat otorisasi untuk autentikasi diberikan, serangan denial of service menyebabkan jaringan, server, atau perantara gagal mengidentifikasi alamat pengirim pengirim. Karena penolakan efek layanan memperlambat server, bisnis harus melakukan analisis data secara menyeluruh.

Man in the middle attack

Peretas atau penyerang, seperti yang ditunjukkan pada Gambar 3, berupaya menguping percakapan yang terjadi antara kedua sistem. Kecerdasan bisnis platform IoT yang digunakan untuk pengumpulan dan transmisi data di cloud sangat dirugikan oleh serangan semacam ini. Mengadopsi Internet of Things untuk tujuan intelijen bisnis dapat menjadi masalah serius bagi perusahaan jika perangkat keras yang digunakan untuk Internet of Things tidak cukup kompatibel dengan sistem intelijen bisnis. Masalah terkait analitik: Mengumpulkan informasi untuk tujuan menganalisisnya dan menarik kesimpulan adalah dasar dari intelijen bisnis. (A. Akbar, A. Khan, F. Carrez, 2017). Platform mana yang mampu menangani volume data yang sangat besar untuk menambahkan data nanti, bergantung pada kebutuhan analitik data berperforma tinggi? Dalam keadaan mendesak, mungkin akan sangat sulit untuk mengelola volume data yang sangat besar yang diperlukan untuk alasan analitis. Privasi dan Keamanan Data: Keamanan informasi pengguna sangat penting untuk meluasnya penggunaan teknologi apa pun. Ada sejumlah potensi kerentanan keamanan yang mungkin berkembang di platform IoT akibat ransomware dan serangan malware lainnya.(Al, 2018). Kehilangan data, akses tidak sah ke informasi sensitif, dan masalah dengan data organisasi yang dapat digunakan untuk intelijen bisnis adalah semua kemungkinan akibat kelemahan keamanan di platform internet of things.

Ancaman dari Cloud: IoT bergantung pada server cloud dan komputasi cloud untuk menyimpan dan mengirimkan data. Data organisasi yang digunakan untuk analisis dapat disusupi jika terjadi serangan cloud. (X. Liu et al, 2018). Server cloud menampung informasi yang relevan dengan intelijen bisnis. Saat server di cloud diserang, server tersebut mungkin mengalami kerusakan atau modifikasi data. Masalah ini mungkin berdampak negatif pada data intelijen bisnis. Kekhawatiran Mengenai Integritas Sistem AI yang Sudah Ada Sebelumnya Organisasi bisnis semakin mengandalkan sistem AI yang sudah ada sebelumnya untuk meningkatkan kecerdasan bisnis mereka, namun sistem ini memiliki kerentanan keamanannya sendiri. Organisasi dapat meningkatkan analisis data mereka dengan bantuan elemen AI yang baru diimplementasikan. Menggabungkan dua sistem dengan karakteristik AI. Penyerang yang sangat jahat mungkin mendapatkan akses ke data analitik organisasi melalui bentuk serangan dalam intelijen bisnis ini.

Permasalahan

Penting untuk dicatat bahwa tidak semua serangan diciptakan sama. Kekhawatiran dengan BI dan Internet of Things meliputi hal-hal berikut. Memahami IoT: Mungkin sulit untuk memahami gagasan Internet of Things karena kompleksitasnya yang melekat. Meningkatkan pengetahuan kita tentang bagaimana platform Internet of Things dapat memengaruhi studi intelijen, aktivitas, dan analisis data perusahaan adalah perhatian utama dalam bidang studi ini. Internet of Things menambah kompleksitas intelijen bisnis dalam hal membuat pilihan berdasarkan informasi dan memproses data secara real time. masalah dengan transfer data: Berbagai jenis teknologi dan koneksi online membentuk tulang punggung web.

Ketika koneksi jaringan atau internet tidak dapat diandalkan atau lamban, masalah koneksi data mungkin muncul. Ketika datang ke catatan perusahaan, volume informasi yang berlebihan dikumpulkan dan diproses untuk dianalisis. Dengan sejumlah besar data yang dikumpulkan dan dibuat setiap hari, bisnis sekarang memiliki sejumlah besar opsi analitis yang dapat mereka gunakan untuk menambang wawasan yang dapat meningkatkan operasi mereka. Pembaruan waktu nyata untuk alat BI dan Internet of Things sangat bergantung pada akses online konstan. Akibatnya, masalah pemrosesan data akan muncul karena koneksi internet yang lamban atau tidak memadai.

Konflik dengan Perangkat Keras Lain: Berbagai sensor digunakan dalam proses pengumpulan data. Internet of Things Gateway, platform Internet of Things yang menggunakan teknologi intelijen bisnis untuk meningkatkan keakuratan data terkait tren pasar yang dapat diidentifikasi dan dianalisis, dihubungkan ke sensor ini. Proliferasi serangan dunia maya seperti ransomware dan malware virus Trojan telah menghambat efektivitas kemampuan keamanan AI bawaan sistem IoT dan BI.

Kehilangan informasi dan jejak kertas: Salah satu bagian terpenting dari setiap perusahaan adalah informasi dan data yang dikumpulkan dan disimpannya. Dalam konteks intelijen bisnis, pengumpulan dan analisis data digunakan untuk meramalkan perkembangan organisasi dan tren pasar. Kumpulan data besar dikumpulkan dan dianalisis untuk keperluan statistik. Dalam hal melindungi informasi perusahaan yang sensitif, platform Internet of Things gagal. Hal ini mempermudah pencuri dan peretas untuk mengawasi data perusahaan Anda. Ini membuka jalan bagi pelaku jahat untuk memodifikasi data perusahaan yang sensitif dan mendatangkan kerugian finansial. Masalahnya berasal dari komitmen goyah platform internet Asia terhadap perlindungan data. Mengidentifikasi Platform IoT Terbaik: Pertimbangan penting harus diberikan pada platform IoT perusahaan yang dipilih. Mengintegrasikan IoT dengan BI adalah upaya yang menantang. Akibatnya, kerangka intelijen bisnis perlu berkembang di masa depan untuk memperhitungkan teknologi baru. Selain itu, masalah keamanan di masa mendatang dapat dipicu oleh pemilihan platform yang

tidak sesuai untuk intelijen bisnis. Masalah dengan Enkripsi Data: Tidak semua solusi yang mendukung IoT memadai untuk mengamankan bisnis. Saat menggunakan strategi intelijen bisnis, informasi dapat dikumpulkan dengan cepat. Beberapa platform IoT intelijen bisnis masih kekurangan mekanisme enkripsi yang kuat, bahkan beberapa dekade setelah pengenalan Internet.

Solusi

Peristiwa kritis pada sistem Internet of Things dapat berdampak buruk pada intelijen bisnis karena beberapa alasan, termasuk berbagai jenis serangan. Situasi dapat diperbaiki dengan penggunaan tindakan pencegahan dan pemeriksaan keselamatan secara teratur. Validasi fungsionalitas dan standar keamanan: Salah satu komponen paling penting dari Internet of Things adalah keamanannya.

Sistem dapat dilindungi dari segala jenis serangan atau bahaya dunia maya dengan penggunaan fitur keamanan berbasis IoT yang diterapkan untuk intelijen bisnis. Inventaris Kargo Aman: Bisnis harus memastikan mereka memiliki tinjauan kode aman. Untuk menurunkan risiko selama penerapan platform IoT untuk analitik bisnis, tinjauan kode yang aman sangat penting. Kerentanan dan bahaya jaringan dapat ditemukan dengan menggunakan metode penetrasi, yang digunakan dalam konteks ini.

Agar berhasil menerapkan intelijen bisnis pada platform Internet of Things, metode penetrasi end-to-end harus digunakan untuk menemukan masalah dan kegagalan jaringan. Seperti yang dikatakan sebelumnya, enkripsi data sangat penting untuk keberhasilan aplikasi intelijen bisnis Internet of Things. Informasi tersebut kemudian dianalisis setelah diolah. Penggunaan enkripsi selama pengumpulan dan pengiriman data melalui jaringan membuat data tersebut lebih aman. Mengenkripsi data akan membuat analisisnya lebih aman. Kriptografi kunci publik dan kunci privat dapat digunakan untuk mencapai hal ini. Terapkan kelas SSL: Internet of Things hanya bergantung pada konektivitas online dan antarmuka pengguna grafis.

Sebagian besar model BI sekarang mengandalkan semacam antarmuka berbasis web untuk memfasilitasi berbagi data. Oleh karena itu, pengguna di lapisan gateway aman kurang terlindungi dari perangkat lunak berbahaya dan ransomware. Gateway menyediakan layanan otorisasi dan otentikasi port dengan memediasi lalu lintas antara server aplikasi dan intranet. Kecerdasan bisnis bergantung pada analisis data berbasis Internet; penerapan BI yang berhasil di perusahaan memerlukan autentikasi server dan port yang kuat.

Kelebihan dan Kekurangan

Berikut ini adalah beberapa manfaat yang dibawa oleh Internet of Things untuk BI perusahaan. Peningkatan output manufaktur dapat dicapai melalui penggunaan sistem Internet of Things (IoT) yang mendukung layanan business intelligence (BI). Meningkatkan output pabrik dimungkinkan melalui peningkatan kapasitas pabrik, ketergantungan, dan efisiensi. Prosedur interaktif yang efektif berdasarkan analisis data operasional dapat meningkatkan efisiensi operasional organisasi. Dengan mempermudah akses ke informasi relevan dari masa lalu, platform IoT memfasilitasi pemantauan data real-time. Peramalan dan manajemen beban dinamis: Manajemen pasokan dan permintaan yang berhasil dapat diterapkan untuk menurunkan beban. Dengan dukungan intelijen bisnis dan Internet of Things, perusahaan dan organisasi dapat mencapai tren pemasaran di masa depan.

Organisasi dapat melindungi diri dari penipuan dan kehilangan keuntungan dengan menggunakan Internet of Things untuk Business Intelligence untuk memantau operasi dan menemukan outlier sebelum menimbulkan masalah. Berikut ini adalah beberapa masalah penggunaan IoT untuk tujuan BI. Karena ketergantungannya pada begitu banyak teknologi yang berbeda, mengintegrasikan platform Internet of Things dengan Business Intelligence

adalah tugas yang sulit. Karena sangat bergantung pada Internet, keamanan dan privasi Internet of Things menjadi sangat penting. Ini berarti bahwa ada kemungkinan besar serangan data. Ketidakcocokan: komponen IoT tertentu tidak dirancang untuk bekerja dengan sistem lain. Langkah-langkah keamanan yang tidak memadai memudahkan peretas untuk mengakses informasi perusahaan yang sensitif.

Pembahasan

"Internet of Things" mengacu pada sistem perangkat elektronik yang saling terhubung, seperti yang ditemukan di bisnis, sistem transportasi, rumah, dan tempat lainnya. Banyak industri mendapat manfaat dari penerapan teknologi IoT; ini mencakup semuanya, mulai dari rumah pintar hingga aplikasi konsumen hingga platform media. Bisnis telah mendapat banyak manfaat dari evolusi cepat IoT dalam beberapa tahun terakhir, karena mereka sekarang dapat menawarkan layanan dan produk baru yang inovatif kepada klien mereka yang memberikan hasil yang nyata.

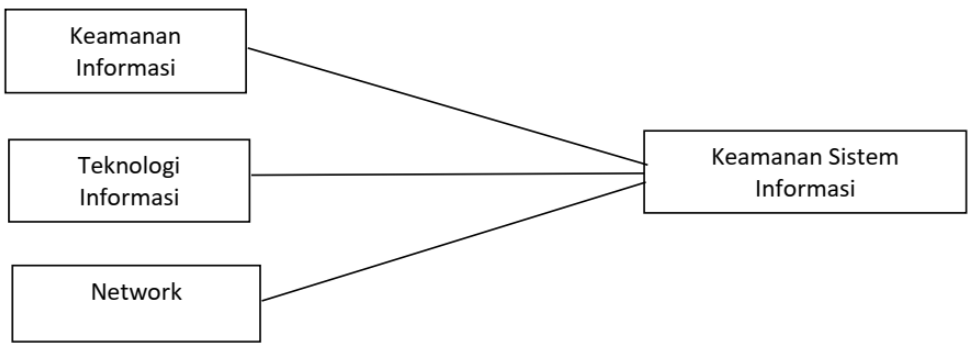
Internet of things juga rentan terhadap serangan seperti denial of service dan man in the middle attack, serta serangan botnet. Serangan Botnet mencakup komunikasi antara beberapa komputer. Dalam konteks serangan botnet, botnet dilepaskan ke dalam jaringan untuk menyerang banyak sistem secara bersamaan. Ini dilakukan dengan tujuan mengganggu tugas operasional rutin atau menurunkan layanan keseluruhan dari sistem target. Permintaan serangan intelijen bisnis di internet sering kali berbentuk pesan teks atau email. Ketika sejumlah besar pengguna mencoba mengakses jaringan sekaligus, waktu respons server meningkat, yang mungkin berdampak negatif pada intelijen bisnis. Kecerdasan bisnis pada platform IoT menghadapi tantangan seperti penolakan serangan layanan. Ketika layanan tidak tersedia pada saat-saat kritis dalam operasi rutin, ini dikenal sebagai denial of service [12]. Ada sejumlah potensi penyebab gangguan layanan.

Serangan denial of service terdistribusi mungkin memiliki konsekuensi yang luas, termasuk kompromi beberapa sistem BI melalui pengenalan file malware. Jika penyerang menyuntikkan kode file berbahaya ke dalam sistem organisasi, itu akan berdampak negatif di mana data tidak dapat diakses oleh karyawan atau bisnis itu sendiri, mencegahnya membuat keputusan strategis yang tepat.

Saat otorisasi untuk autentikasi diberikan, serangan denial of service menyebabkan jaringan, server, atau perantara gagal mengidentifikasi alamat pengirim pengirim. Karena penolakan efek layanan memperlambat server, bisnis harus melakukan analisis data secara menyeluruh. Tujuan Man in the Middle Attack adalah menguping data yang dikirim antara dua jaringan terpisah. Apa yang kita miliki di sini adalah serangan terhadap IoT.

Konseptual Framework

Berdasarkan rumusan masalah, kajian teori, dan penelitian terdahulu maka diperoleh kerangka berfikir artikel ini seperti berikut.



Berdasarkan gambar konseptual framework di atas, maka : Keamanan Informasi, Teknologi Informasi, dan Network berpengaruh terhadap Keamanan Sistem Informasi.

KESIMPULAN

Studi ini mengklaim telah mengatasi sejumlah masalah dan kesulitan yang dihadapi oleh sistem BI berbasis internet. Berbagai serangan pada platform IoT dijelaskan, bersama dengan referensi literatur yang relevan. Perspektif tentang banyak masalah keamanan informasi dan solusi yang diusulkan untuk platform Internet of Things dibahas. Sebagai kesimpulan, dibahas manfaat dan kelemahan utama IoT untuk BI.

REFERENSI

A. Akbar, A. Khan, F. Carrez, dan K. M. (2017). Predictive analytics for complex IoT data streams. *IEEE Internet Things J*, *4*, 1571–1582.

Al, F. C. et. (2018). Real-Time Probabilistic Data Fusion for Large-Scale IoT Applications. *" IEEE Access*, *6*, 10015–10027.

D. Goel, S. Chaudhury, dan H. G. (2017). *An IoT approach for context-aware smart traffic management using ontology*. 42–49.

F. Bromberg, D. Dujovne, T. Watteyne, A. L. Diedrichs, dan K. B.-L. (2018). Prediction of Frost Events Using Machine Learning and IoT Sensing Devices. *IEEE Internet Things J*, 4589–4597.

Fuada, S., Setyowati, E., Aulia, G. I., & Riani, D. W. (2023). Narative Review Pemanfaatan Internet-of-Things Untuk Aplikasi Seed Monitoring and Management System Pada Media Tanaman Hidroponik Di Indonesia. *INFOTECH Journal*, *9*(1), 38–45. https://doi.org/10.31949/infotech.v9i1.4439

Internet, P., Things, O. F., Analisa, D., & Dan, D. (2023). *SmartAI*. 1–8.

Munawa, Z., & Putri, N. I. (2020). Keamanan IoT Dengan Deep Learning dan Teknologi Big Data. *Tematik : Jurnal Teknologi Informasi Komunikasi (e-Journal)*, *7*(2), 161–185. https://jurnal.plb.ac.id/index.php/tematik/article/view/479

Nohuz, E., Alaboud, M., El-Drayi, B., Tamburro, S., Kachkach, S., & Varga, J. (2014). Demons-Meigs pseudosyndrome mimicking the symptoms of pregnancy: A case report. *Journal of Reproduction and Infertility*, *15*(4), 229–232.

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi : Keamanan Informasi , Teknologi Informasi Dan Network (Literature Review Sim). *Jurnal Ekonomi Manajemen Sistem Informasi (Jemsi)*, *Vol. 3*(No. 5), 564–573.

Rozi, F. (2020). Systematic Literature Review pada Analisis Prediktif dengan IoT: Tren Riset, Metode, dan Arsitektur. *Jurnal Sistem Cerdas*, *3*(1), 43–53. https://doi.org/10.37396/jsc.v3i1.53

Turyadi, I. U. (2021). Analisa Dukungan Internet of Things (IoT) terhadap Peran Intelejen dalam Pengamanan Daerah Maritim Indonesia Wilayah Timur. *Jurnal Teknologi Dan Manajemen Informatika*, *7*(1), 29–39. https://doi.org/10.26905/jtmi.v7i1.6040

X. Liu et al. (2018). *Application of Temperature Prediction Based on Neural Network in Intrusion Detection of IoT*.