PENTINGNYA KEAMANAN DATA DALAM INTELIJEN BISNIS

Novianti Indah Putri[1] , Rita Komalasari[2], Zen Munawar[3]

1. Teknik Informatika, Fakultas Teknologi Informasi Universitas Bale Bandung
2. Manajemen Informatika, Politeknik LP3I Bandung
3. Manajemen Informatika, Politeknik LP3I Bandung

ABSTRACT

The internet of things is a revolution in the business field and the adoption of IoT devices in business organizations leads to business data management in line with the organization. The application of a business intelligence system is a technical and social solution to facilitate communication and accelerate easy access to information. but business dependence is increasing on information systems; technical, non-technical damage, threats and actions that violate the principles of business information security. The main objective of this research is to determine the data security of the implementation of a business intelligence system. Data is the greatest asset of a business organization and the proper maintenance of data is the main concern of every organization. The internet of things is used in every business sector for efficient data utilization and is expected to enrich data from the use of the devices used. Data security issues are the biggest concern in business and data matters. Business intelligence continues to rely on historical and present data to predict and perform calculations on future data. Due to data security concerns, data organizations can be in danger due to potential threats, data loss, and data manipulation. Trusted business intelligence on plugins requiring internet connectivity. The attacker works on the browser system and destroys the plugins associated with it, if the browser cannot be protected from antivirus and firewall. Lack of device security features would allow attackers to track system details and manipulate systems or data. With data security, it can ensure continuity of operations and reduce damage and cyber threats so as to increase investment opportunities through the development of new markets.

Key Word: Data security, business intelligence, business systems, internet of things

ABSTRAK

Internet of things merupakan revolusi di bidang bisnis dan adopsi perangkat IoT dalam organisasi bisnis mengarah pada keberhasilan pengelolaan data bisnis seiring dengan keberhasilan organisasi. Penerapan sistem Intelijen bisnis merupakan solusi teknis dan sosial untuk memfasilitasi komunikasi dan mempercepat akses informasi yang mudah. tetapi ketergantungan bisnis meningkat pada sistem informasi; mengakibatkan kerusakan teknis, non-teknis, ancaman dan tindakan yang melanggar prinsip keamanan informasi bisnis. Tujuan utama dari penelitian ini adalah untuk mengetahui keamanan data terhadap implementasi sistem intelijen bisnis.. Data adalah aset terbesar dari setiap organisasi bisnis dan pemeliharaan data yang tepat adalah perhatian utama setiap organisasi. Internet of things digunakan di setiap sektor bisnis untuk pemanfaatan data yang efisien dan organisasi diharapkan dapat memperkaya data dari penggunaan perangkat yang digunakan. Masalah keamanan data menjadi perhatian terbesar dalam mengelola dan memelihara data bisnis. Intelijen bisnis dipertahankan tergantung pada data historis dan sekarang untuk memperkirakan dan melakukan perhitungan pada data masa depan. Karena masalah keamanan data, data organisasi dapat berada dalam bahaya karena potensi ancaman, kehilangan data, dan manipulasi data. Intelijen bisnis terutama bergantung pada plugin yang membutuhkan konektivitas internet. Penyerang dapat bekerja di browser sistem dan menghancurkan plugin yang terkait dengannya, jika browser tidak dilindungi dari antivirus dan firewall. Kurangnya fitur keamanan perangkat akan memungkinkan penyerang melacak detail sistem dan melakukan serangan dengan memanipulasi atau mencuri data. Dengan keamanan data maka dapat dipastikan kelangsungan operasi dan mengurangi kerusakan dan ancaman dunia maya sehingga dapat meningkatkan peluang investasi melalui pengembangan pasar baru.

Kata Kunci: Keamanan data, intelijen bisnis, sistem bisnis, internet of things

1. PENDAHULUAN

Intelijen bisnis adalah teknologi yang sedang berkembang di industri bisnis yang menggunakan pendekatan proses berbasis teknologi untuk membuat perencanaan dan keputusan strategis. Intelijen bisnis membantu dalam menganalisis data dan informasi untuk membantu eksekutif bisnis dan manajer dalam membuat keputusan bisnis yang efektif.

Intelijen bisnis terdiri dari penggunaan berbagai alat dan metode yang memungkinkan dan membantu dan organisasi dalam pengumpulan data dan informasi yang relevan dari sumber internal dan sumber eksternal. Internet of Thing banyak digunakan dalam proses Intelijen bisnis untuk membuat keputusan strategis dan membuat perencanaan yang efektif. *Internet of things* memungkinkan karyawan yang bekerja di organisasi untuk terhubung ke beberapa perangkat yang beroperasi di jaringan yang sama. Implementasi perangkat *internet of things* di sektor bisnis memberikan keuntungan yang sangat besar dalam pengelolaan dan perencanaan operasi bisnis. Mempertimbangkan keunggulan *internet of things* dalam intelijen bisnis, terlihat bahwa *internet of things* sangat efektif dalam mengestimasi dan mengevaluasi penjualan serta memahami strategi pasar. Penelitian sebelumnya sudah menyelidiki apakah ada efek signifikan dalam keakuratan model prediktif yang efektif [1]. Kegiatan operasional bisnis dapat ditingkatkan dengan penerapan *internet of things* di industri bisnis. Dalam hal intelijen bisnis, *internet of things* bisa sangat efektif dan tidak efisien dalam pemanfaatan data dan informasi untuk membantu karyawan manajemen puncak mendapatkan data yang diperkaya untuk membuat rencana atau strategi bisnis. Intelijen bisnis pada dasarnya bergantung pada fakta bahwa, ia menggunakan data sekarang dan data historis untuk membedakan perubahan dan kemajuan. *Internet of things* sangat efektif dalam melakukan penghitungan dan estimasi data masa depan organisasi bisnis. *Big data* dan komputasi awan banyak digunakan dalam intelijen bisnis dan telah menciptakan dampak yang signifikan pada peningkatan intelijen bisnis. *Internet of things* didukung oleh jaringan komputasi awan sehingga berdampak besar pada Intelijen bisnis dengan penggunaan *big data* dengan mengidentifikasi, menganalisis dan menemukan data yang terkait dengan bisnis.

Internet of things menggunakan kumpulan data dari berbagai sumber dan bisa internal maupun eksternal. Beberapa jenis masalah dan tantangan dapat terjadi di dalam organisasi ketika platform *internet of things* digunakan untuk intelijen bisnis. Tantangan keamanan dan ancaman lainnya akan dibahas di bagian ini. Solusi untuk berbagai jenis tantangan keamanan data, masalah dan ancaman juga akan dijelaskan dalam bagian berikutnya. Kelebihan dan kekurangan terkait Intelijen bisnis akan dibahas di bagian ini. Bagian akhir akan di bahas mengenai kesimpulan hasil paparan yang telah disampaikan sebelumnya.

2. KAJIAN TEORITIS

Internet of things adalah jaringan perangkat yang terhubung secara fisik yang digunakan dalam organisasi bisnis, kendaraan, peralatan rumah tangga dll [2]. Ini terutama terdiri dari perangkat lunak, sensor, konektivitas, dan aktuator. Seperti yang telah penulis jelaskan bahwa kombinasi komponen tersebut dengan konektivitas internet membantu dalam pertukaran data dan informasi. Ini dapat digunakan untuk tujuan melakukan operasi atau tugas tertentu. *Internet of things* memiliki cakupan implikasi penerapan di setiap sektor. Contoh penarapannya dapat digunakan untuk implementasi rumah pintar, aplikasi konsumen, aplikasi media, dll. *Internet of things* adalah penggunaan perangkat yang terhubung secara cerdas [3]. Perangkat yang terhubung tertanam dengan aktuator dan sensor serta berbagai perangkat fisik lainnya untuk memanfaatkan data. *Internet of things* telah berkembang pesat selama beberapa tahun terakhir untuk memberikan dimensi baru bagi organisasi dan industri bisnis dan sangat efektif untuk memberikan solusi kepada pelanggan untuk peningkatan drastis dan dramatis dari efisiensi energi, pendidikan, kesehatan dan

keamanan proses bisnis kehidupan manusia dan standar hidup. Platform *internet of things* dapat mengintegrasikan data dari beberapa perangkat dan untuk menerapkan analitik pada data yang dikumpulkan terintegrasi untuk dibagikan untuk tujuan berbagi data dan sangat efektif untuk mengidentifikasi data apa yang akan diterima dan data apa yang perlu diabaikan.

Karakteristik utama dari platform *internet of things* berguna untuk menghubungkan segala sesuatu dalam komunikasi global dan struktur informasi [4]. Platform perangkat yang ada dan digunakan heterogen karena bergantung pada jaringan dan platform perangkat keras yang berbedadan sangat efektif dalam memberikan keamanan data dan informasi.

Cakupan penerapan *internet of things* di dunia nyata sangatlah besar [5] digunakan oleh organisasi bisnis, industri atau oleh manusia untuk mendapatkan hasil yang dinamis. *Internet of things* membuat revolusi besar untuk membuat Rumah Pintar [5]. Pendekatan rumah pintar akan populer dan akan umum seperti *smartphone* dalam beberapa tahun terakhir. Produk *wearable* dikembangkan dan dibuat dari platform *internet of things* membuat ledakan besar di pasar saat ini. Produk *wearable* terintegrasi dan tertanam dengan perangkat lunak dan sensor yang terutama digunakan untuk pengumpulan informasi dan data pengguna. Data dan informasi yang telah dikumpulkan kemudian di proses untuk mengekstraksi wawasan pengguna. Fitur aplikasi lainnya adalah mobil yang terhubung. Mobil secara ekstensif menggunakan keunggulan teknologi *internet of things* untuk mengoptimalkan fungsionalitas internal kendaraan. Industri *internet of things* mendorong para insinyur dengan perangkat lunak, analisis *big data*, sensor, dll. Untuk membuat dan mengembangkan mesin canggih dengan fitur berkualitas. Contoh penerapan fitur aplikasi lain adalah kota pintar, di bidang pertanian, ritel pintar untuk manajemen energi, dalam perawatan kesehatan, dll [6], *Internet of things* digunakan secara luas untuk intelijen bisnis. Intelijen bisnis adalah proses yang lebih cenderung didorong oleh teknologi untuk tujuan menganalisis data dan menyajikan informasi yang dapat ditindaklanjuti untuk membantu para manajer, eksekutif, dan perusahaan terkait lainnya. untuk membuat keputusan bisnis yang terinformasi [6].

Tujuan utama penggunaan intelijen bisnis dalam suatu organisasi adalah untuk analisis data. Dengan intelijen bisnis dapat memberikan keuntungan yang sangat besar bagi organisasi bisnis untuk meningkatkan efektifitas intelijen bisnis. Efektif dalam mencapai keunggulan kompetitif atas persaingan bisnis dan menghasilkan pendapatan baru. Intelijen bisnis memanfaatkan layanan dan perangkat lunak untuk transformasi data ke dalam bentuk intelijen yang dapat ditindaklanjuti yang membantu organisasi dalam membuat keputusan penting dan kompleks untuk bisnis.

Penggunaan *internet of things* untuk intelijen bisnis membantu dalam menciptakan Dasbor Intelijen Bisnis untuk organisasi bisnis. Terdapat beberapa alasan penggabungan intelijen bisnis dalam organisasi [7], dapat membantu organisasi dalam melacak dan memantau data real-time dan juga dapat digunakan untuk tujuan berbagi data realtime untuk membuat keputusan yang lebih baik terkait bisnis [7].

Penerapan platform *internet of things* untuk Intelijen bisnis meningkatkan sensor dari operasi bisnis. Sesuai penulis, kemajuan terbaru dalam teknologi membantu organisasi untuk mengumpulkan banyak data di dunia berbasis data, terutama saat penggunaan data dalam bidang e-commerce dengan menggunakan sistem rekomendasi. Sistem rekomendasi diperlukan karena sebelumnya terdapat kelemahan pada sistem berbasis konten [8].

Informasi atau data yang dikumpulkan dapat diubah dengan mudah menjadi format yang dapat dibaca dengan bantuan alat intelijen bisnis. Selain itu, Intelijen bisnis juga sangat efisien dalam menganalisis dan memelihara informasi terkini. Efektif dalam membuat pengumpulan data cepat dan pemrosesan waktu nyata serta pengumpulan data. Intelijen bisnis terkait dengan konsep *big data*. Salah satu contoh penggunaan *big data* adalah pada e-commerce. Secara komersial, e-commerce dapat disebut sebagai kegiatan yang berusaha menciptakan transaksi yang panjang antara perusahaan dan individu [9].

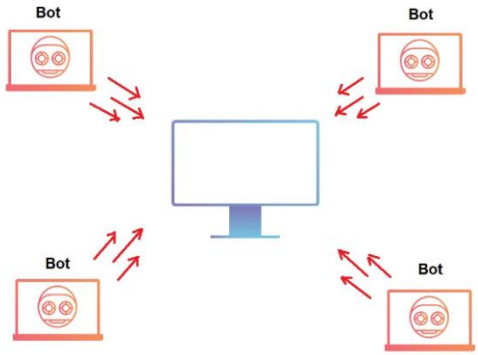
Big data berfokus pada informasi yang rumit dan analitik data. Intelijen bisnis juga memfokuskan pada analisis kumpulan data di berbagai bidang seperti alat canggih, aplikasi perangkat lunak, dan infrastruktur. *Internet of things* sangat penting bagi organisasi untuk membangun komunikasi antara berbagai jenis sumber dan produk seperti sensor, teknologi yang dapat dikenakan, dan perangkat.

3. JENIS SERANGAN PADA INTELIJEN BISNIS

Serangan bisa dari beberapa jenis. Masalah keamanan dan privasi di platform *internet of things*, serangan dilakukan. Serangan dapat dilakukan oleh peretas, penyusup, dan agen tidak sah. Serangan dapat berupa serangan siber fisik, serangan siber jaringan, serangan perangkat lunak, dan serangan siber. serangan enkripsi [7]. Alasan utama serangan fisik adalah karena adanya sensor di perangkat *internet of things*. Peretas umumnya mencoba mengakses sistem pengguna yang terletak dekat dengan jarak dekat [7]. Gangguan akan membantu peretas atau penyusup untuk mengekstrak data yang diinfuskan dengan kode berbahaya. Dalam serangan jaringan siber, peretas atau penyusup mencoba mengakses jaringan pengguna untuk mengidentifikasi dan memeriksa data apa yang sebenarnya mengalir di jaringan. Dunia saat ini tidak lepas dari peran data karena semua dibangun di atas sebuah fondasi data [10]. Contoh paling umum dari serangan siber Jaringan adalah serangan *man-in-the middle*. Selain serangan jaringan siber, serangan lain adalah serangan perangkat lunak. Dalam konteks serangan perangkat lunak, file berbahaya atau *malware* disuntikkan ke pengguna untuk melacak dan memantau data sistem pengguna dan juga untuk melacak aliran data. Serangan perangkat lunak dapat merusak data atau file dengan memasukkan virus. Jenis serangan terakhir yang dijelaskan oleh penulis adalah serangan enkripsi. Dalam konteks serangan enkripsi, penyusup atau peretas menyimpulkan kunci enkripsi untuk membuat kode dan algoritme mereka sendiri untuk membuka kunci enkripsi. Sesuai penulis, setelah peretas dapat membuka kunci, mereka memasukkan kode mereka sendiri ke dalam sistem pengguna untuk memantau sistem. Sesuai penulis berdasarkan jenis serangannya, dapat berupa DDoS (*Distributed Denial of services*, Bonnets, *Man in the Middle attack*, dll.

3.1 Botnet Attacks

Botnet adalah koneksi dari satu atau lebih perangkat [11]. Dalam konteks serangan Botnet, umumnya dipraktekkan dengan maksud untuk mengganggu pekerjaan operasi normal atau dapat digunakan untuk degradasi layanan keseluruhan dari sistem target [11]. Untuk pembuatannya, sejumlah besar Botnet diperlukan sebelum menginisialisasi serangan. Seperti yang ditunjukkan pada gambar 1, setelah serangan diinisialisasi, botnet6 dikirim ke jaringan untuk menargetkan sistem dalam skala besar. Permintaan penyerangan di *internet of things* untuk intelijen bisnis datang dalam bentuk pesan atau email. Jenis serangan dapat menimbulkan dampak buruk pada intelijen bisnis dengan memperlambat server jaringan dengan membuat jaringan sibuk bagi pengguna untuk mengakses jaringan dengan membekukan sementara server.

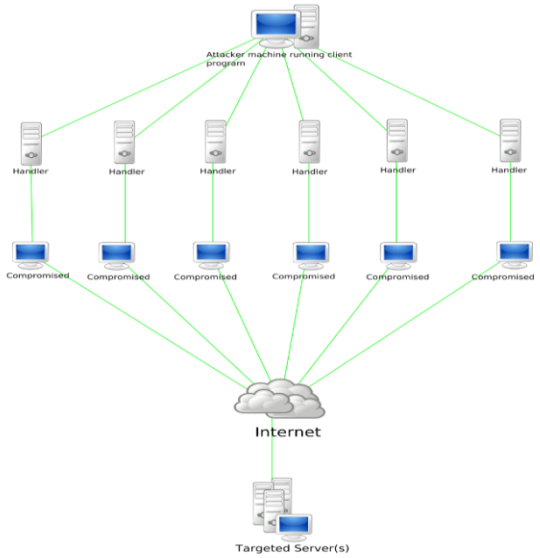


Gambar 3.1.: Jenis serangan yang paling umum dari serangan Botnet adalah Distributed Denial of service attack (DDoS).

3.2 Denial of Service

Denial of service attack merupakan masalah lain yang menjadi perhatian dalam aspek intelijen bisnis di platform *internet of things*. Penolakan layanan terjadi ketika tidak adanya layanan yang terjadi selama proses kerja biasa [12]. Tidak tersedianya layanan dapat terjadi karena berbagai alasan. Dalam konteks serangan penolakan layanan terdistribusi, sejumlah besar sistem komputer yang digunakan untuk intelijen bisnis mungkin terpengaruh dengan memperkenalkan file berbahaya dalam sistem organisasi. Seperti yang ditunjukkan oleh gambar 2, penyerang menyuntikkan kode file berbahaya ke dalam

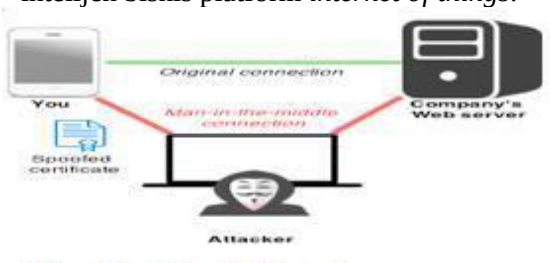
sistem organisasi akan menimbulkan dampak buruk di mana itu akan membuat data tidak dapat diakses oleh karyawan atau organisasi bisnis untuk analisis yang tepat dan membuat keputusan strategis. Serangan penolakan layanan, jaringan, jaringan atau server tidak dapat menemukan alamat balik dari peretas atau penyerang saat mengirimkan persetujuan untuk otentikasi. Hal tersebut menjadikan organisasi bisnis untuk membuat analisis data yang tepat karena pengaruh *denial of service* membuat server berjalan lambat.



Gambar 3.2. Denial of Service [13]

3.3 Man in the middle attack.

Gambar 3 menunjukkan, para hacker atau penyerang mencoba untuk mencegat komunikasi yang terjadi antara dua sistem [13]. Serangan semacam itu memiliki dampak yang sangat merugikan pada intelijen bisnis platform *internet of things*.



Gambar 3.3. Para peretas atau penyerang mencoba mencegat komunikasi yang terjadi antara dua sistem. [14]

Gambar 3. Para peretas atau penyerang mencoba mencegat komunikasi yang terjadi antara dua sistem. Jenis serangan dalam intelijen bisnis dapat mengakibatkan penyerang yang sangat berbahaya memiliki kendali penuh atas sistem pengguna untuk memanipulasi dan mengubah data analitis organisasi bisnis.

4 . SOLUSI KEAMANAN

4.1 Permasalahan

Bergantung pada jenis serangan yang berbeda, mungkin ada beberapa jenis masalah yang mungkin terjadi. Masalah terkait *internet of things* dalam Intelijen bisnis adalah sebagai berikut.

Memahami *internet of things*: Konsep *internet of things* sangat kompleks dan masalah dengan pemahaman konsep internet of things dapat terjadi. Masalah utama yang terkait dengan *internet of things* di sektor intelijen bisnis adalah tentang meningkatkan kemampuan pemahaman untuk perubahan dan implikasi yang dibuat dalam platform *internet of things* untuk meningkatkan intelijen bisnis, aktivitas, dan survei analitik data [14]. Pemahaman yang tidak tepat tentang *internet of things*, membuat intelijen bisnis lebih kompleks untuk membuat keputusan yang tepat dan untuk memproses data aktual dan *real-time*.

Masalah dengan Konektivitas Data: Internet bergantung pada beberapa teknologi dan konektivitas internet. Masalah dengan masalah konektivitas data dapat terjadi jika jaringan dan konektivitas internet tidak akan tersedia atau lambat. Dalam konteks intelijen bisnis, sejumlah besar data dikumpulkan dan dikumpulkan untuk memproses data untuk analisis. Saat ini, sejumlah besar data yang dikumpulkan dan dihasilkan setiap hari menawarkan berbagai peluang analitis bagi organisasi untuk mengungkap informasi yang bermanfaat untuk operasinya [15]. Dalam konteks intelijen bisnis, pembaruan instan diperlukan dan *internet of things* sepenuhnya bergantung pada konektivitas internet. Oleh karena itu, koneksi internet yang lambat dan konektivitas internet yang tidak tersedia akan menimbulkan masalah saat memproses data.

Masalah dengan kompatibilitas perangkat keras: Proses pengambilan data terjadi melalui berbagai jenis sensor. Sensor ini terhubung ke *gateway internet of things*

untuk pengumpulan dan transmisi data di cloud [12]. Adopsi *internet of things* untuk tujuan intelijen bisnis dapat menjadi situasi kritis dari suatu masalah dalam organisasi bisnis jika perangkat keras perangkat *internet of things* digunakan terlalu kompatibel untuk mendukung sistem Intelijen bisnis.

Masalah yang terkait dengan analitik: Intelijen bisnis sepenuhnya didasarkan pada pengumpulan data yang akan diproses untuk wawasan yang dapat ditindaklanjuti. Tergantung pada permintaan platform analitik data berkinerja tinggi, mana yang cukup mampu menangani data dalam jumlah besar untuk menambahkan data di lain waktu? Mengelola data dalam jumlah besar untuk tujuan analisis juga bisa menjadi masalah besar selama situasi kritis.

Masalah Keamanan Data: Keamanan data adalah masalah utama untuk adopsi semua jenis teknologi. Karena terjadinya serangan *ransomware* dan serangan malware lainnya, ada beberapa jenis masalah keamanan yang mungkin muncul di platform IoT. Masalah keamanan di platform *internet of things* dapat menyebabkan hilangnya data, pemantauan atau pelacakan data organisasi yang dapat digunakan untuk tujuan Intelijen bisnis dan jenis data dan masalah terkait perangkat keras lainnya dapat terjadi dengan masalah keamanan terkait data.

Cloud Attacks: *Internet of things* menggunakan komputasi awan dan server awan untuk penyimpanan dan transmisi data. Dalam konteks serangan *cloud*, data yang disimpan di server oleh organisasi untuk tujuan analisis data mungkin terpengaruh. Data yang terkait dengan intelijen bisnis disimpan di dalam server awan. Serangan *cloud* di server akan menyebabkan perubahan atau manipulasi data di server *cloud*. Masalah tersebut dapat menimbulkan efek buruk pada data yang terkait dengan intelijen Bisnis.

Masalah Keamanan dalam AI *Built*: Kecerdasan buatan mengambil bentuk baru dalam dunia bisnis dan organisasi bisnis menggunakan teknologi *built-in* AI untuk meningkatkan intelijen bisnis. Pengenalan fitur AI membantu organisasi dalam analisis data yang lebih baik.

Mengintegrasikan fitur AI ke dalam platform *internet of things* membuat intelijen bisnis membuat identifikasi dan analisis data lebih tepat sehubungan dengan tren pasar [14].

Maraknya berbagai jenis serangan dunia maya seperti serangan ransomware, serangan malware melalui virus Trojan, dll. Menciptakan masalah serius dalam fitur keamanan AI yang dibangun, sehingga berdampak buruk pada platform *internet of things* dan intelijen bisnis juga. Kebocoran informasi dan jejak informasi: Data dan informasi adalah salah satu komponen utama dari setiap organisasi bisnis. Dalam konteks intelijen bisnis, pertumbuhan organisasi dan tren bisnis masa depan dianalisis dengan mengumpulkan data yang terkait dengan bisnis tersebut. Sejumlah besar data dikumpulkan dan diproses untuk tujuan analisis data. Kekurangan fitur keamanan pada platform *internet of things* akan memungkinkan penyerang atau peretas memiliki akses pada data bisnis. Ini akan memudahkan peretas atau penyusup untuk melacak dan memantau data yang terkait dengan bisnis. Ini akan membantu agen yang tidak sah, atau peretas atas memanipulasi data yang terkait dengan bisnis dan dapat membawa kerugian finansial bagi organisasi.

Kurangnya keamanan di platform *internet of things* menyebabkan jenis masalah seperti itu. Pemilihan platform *internet of things* yang Tepat: Pemilihan platform *internet of things* yang Tepat untuk organisasi bisnis sangat penting. Penerapan IoT dalam intelijen bisnis sangat kompleks. Oleh karena itu, perubahan teknologi di masa depan mengarah pada perubahan model intelijen bisnis secara keseluruhan. Pemilihan platform yang tidak tepat untuk intelijen bisnis juga dapat menimbulkan masalah keamanan dalam waktu dekat.

Masalah Enkripsi Data: Ada beberapa jenis alat yang didukung *internet of things* yang tidak cukup mampu untuk mengenkripsi bisnis. Ada laju aliran data yang tinggi terjadi dalam pendekatan intelijen bisnis. Bahkan setelah penggunaan internet, ada beberapa platform *internet of things* untuk intelijen bisnis yang tidak dapat mengenkripsi data dengan baik dalam hal intelijen bisnis.

4.2 Solusi

Karena beberapa jenis serangan, ada jenis masalah utama yang mungkin terjadi di platform *internet of things* yang menimbulkan efek buruk pada intelijen Bisnis. Tindakan pencegahan dan pemeliharaan langkah-langkah keamanan akan membantu dalam mengurangi masalah tersebut.

Persyaratan keamanan yang tepat dan verifikasi fungsi: Keamanan adalah salah satu aspek utama IoT yang sangat penting untuk membuat fungsi tersebut berfungsi dengan baik.

Penerapan fitur keamanan pada platform IoT untuk Intelijen bisnis akan membuat sistem aman untuk mencegah sistem dari segala jenis serangan siber dan ancaman.

Peninjauan yang aman atas barang: Organisasi bisnis wajib memelihara peninjauan kode yang aman. Penerapan platform IoT untuk intelijen bisnis memerlukan tinjauan kode yang aman untuk meminimalkan tingkat ancaman.

Penerapan Teknik Penetrasi: Teknik penetrasi sangatlah penting untuk mengidentifikasi kerentanan atau ancaman melalui jaringan. Teknik penetrasi ujung ke ujung akan membantu dalam menemukan bug dan kesalahan dalam jaringan untuk implementasi yang efektif dari intelijen bisnis di platform *internet of things*.

Enkripsi Data: Seperti yang telah dibahas, Penerapan Intelijen bisnis pada platform *internet of things* sepenuhnya bergantung pada data. Data yang telah terkumpul kemudian di proses untuk dianalisa. Enkripsi data akan meningkatkan fitur keamanan data selama pengumpulan atau transmisi melalui Jaringan

Enkripsi data akan membuat data lebih aman untuk analisis data. Ini dapat diimplementasikan dengan teknik kriptografi dengan menggunakan kunci publik dan enkripsi kunci privat.

Penggunaan Lapisan Soket Aman: IoT sepenuhnya bergantung pada konektivitas jaringan dan antarmuka web. Di sebagian besar model intelijen bisnis, pertukaran informasi terjadi melalui antarmuka web. Oleh karena itu, pengguna lapisan soket aman akan mengurangi perlindungan data dari serangan *malware* atau ransomware.

Otorisasi dan Otentikasi Gateway: Gateway adalah jembatan yang ada antara server aplikasi dan jaringan lokal yang terhubung ke internet. Dalam konteks Intelijen bisnis, analisis data terjadi melalui internet. Ada otentikasi yang tepat dari server dan gateway akan efektif untuk implementasi yang tepat dari Intelijen bisnis dalam organisasi.

5 KELEBIHAN DAN KEKURANGAN

Keunggulan *internet of things* dalam Intelijen bisnis adalah sebagai berikut. Mengoptimalkan kinerja aset: Implementasi dan adopsi platform *internet of things* untuk intelijen bisnis sangat efektif untuk mengidentifikasi potensi masalah. Kinerja aset dapat ditingkatkan dengan meningkatkan kapasitas, keandalan, dan kapasitas aset.

Meningkatkan efisiensi operasional: efisiensi operasional organisasi dapat ditingkatkan dengan proses interaksi yang efektif dengan menganalisis data operasional. Adopsi platform *internet of things* membantu dalam memantau data real-time dengan menyediakan akses yang jelas ke data historis.

Manajemen beban dan peramalan dinamis: Manajemen permintaan yang sukses dan operasi pasokan dapat ditetapkan untuk mengurangi beban. Bisnis masa depan dan tren pemasaran organisasi dapat dicapai melalui intelijen bisnis dengan penerapan *internet of things*.

Manajemen Fraud dan Pencegahan atas hilangnya Utilitas: Anomali dalam aktivitas bisnis dapat ditentukan untuk mencegah hilangnya utilitas dan manajemen penipuan dapat dicapai dengan penerapan *internet of things* untuk Intelijen bisnis dalam organisasi.

Kekurangan IoT dalam Intelijen bisnis adalah sebagai berikut.

Kompleksitas: IoT sangat kompleks dan untuk mengintegrasikan platform *internet of things* dengan intelijen bisnis akan sangat kompleks karena bergantung pada beberapa teknologi.

Keamanan dan Privasi: Keamanan dan privasi adalah perhatian utama di *internet of things* karena sepenuhnya bergantung pada internet. Oleh karena itu, kemungkinan besar serangan data akan terjadi.

Kompatibilitas: Tidak semua komponen *internet of things* cukup kompatibel untuk mematuhi teknologi lain. Keamanan: Kurangnya fitur keamanan akan memungkinkan peretas di jaringan untuk meretas data organisasi.

6KESIMPULAN

Sesuai makalah tersebut, beberapa masalah dan tantangan terkait intelijen bisnis di platform *internet of things* telah dibahas. Sebuah studi literature dan latar belakang telah disediakan dengan menekankan berbagai jenis serangan pada platform *internet of things*. Penelitian ini telah membahas aspek beberapa masalah dan solusi keamanan data dalam intelijen bisnis dalam platform *internet of things* di ikuti oleh penelitian masa depan. Terakhir, kelebihan utama dan kekurangan dari *internet of things* untuk intelijen bisnis telah tersampaikan.

DAFTAR PUSTAKA

[1] Z. Munawar, "Penggunaan Profil Media Sosial Untuk Memprediksi Kepribadian," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 4, no. 2 SE-Articles, Dec. 2017.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] S. Dieter Tebje Kelly, "Towards the Implementation of IoT forEnvironmental Condition Monitoring in Homes," *IEEE Sens. J.*, vol. 13, no. 10, pp. 3846–3853, 2015.

[4] M. T. Lazarescu, "Design of a WSN platform for long-term environmental monitoring for IoT applications," *IEEE J. Emerg. Sel. Top. Circuits Syst.*, vol. 3, no. 1, pp. 45–54, 2013.

[5] D. Soumya Kanti, C. Bonnet, and N. Nikaein, "An IoT gateway centric architecture to provide novel M2M services," in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, 2014, vol. IEEE World, no. 2, pp. 514–519.

[6] S. Leminen, M. Westerlund, M. Rajahonka, and R. Siuruainen, "Towards IOT Ecosystems and Business Models," *Smart Spaces, Next Gener. Netw.*, vol. 01, pp. 15–26, 2012.

[7] D. Larson and V. Chang, "A review and future direction of agile, business intelligence, analytics and data science," *Int. J. Inf. Manage.*, vol. 36, no. 5, pp. 700–710, 2016.

[8] Z. Munawar, N. Suryana, Z. B. Sa'aya, and Y. Herdiana, "Framework With An Approach To The User As An Evaluation For The Recommender Systems," in *2020 Fifth International Conference on Informatics and Computing (ICIC)*, 2020, pp. 1–5.

[9] Z. Munawar, "Keamanan Pada E-Commerce Usaha Kecil dan Menengah," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 5, no. 1 SE-Articles, Jun. 2018.

[10] Z. Munawar, B. Siswoyo, and N. S. Herman, "Machine learning approach for analysis of social media," *ADRI Int. Journal. Information. Technol.*, vol. 1, pp. 5–8, 2017.

[11] E. Bertino and N. Islam, "Botnets and internet of things security," *Computer (Long. Beach. Calif).*, vol. 50, no. 02, pp. 76–79, 2017.

[12] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[13] K. Zhao and L. Ge, "A survey on the internet of things security," in *Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013*, 2013, pp. 663–667.

[14] T. H. Davenport, "Business Intelligence and Organizational Decisions," *Int. J. Bus. Intell. Res.*, vol. 1, no. 1, pp. 1–12, 2010.

[15] N. I. Munawar, Zen and Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *J-SIKA| J. Sist. Inf. Karya Anak Bangsa*, vol. 02, no. 01, pp. 14–20, 2020.