KEAMANAN IOT DENGAN DEEP LEARNING DAN TEKNOLOGI BIG DATA

Zen Munawar, Novianti Indah Putri[1]
Manajemen Informatika, Teknik Informatika[1]
Politeknik LP3I Bandung, Universitas Bale Bandung[1]
e-mail:munawarzen@gmail.com, noviantiindahputri@gmail.com[1]

Abstrak : Saat ini dalam kehidupan manusia sangat tergantung dengan teknologi , apalagi ditunjang dengan perkembangan dari *Internet of Things* (IoT), yang memungkinkan komunikasi dan interaksi dengan berbagai perangkat. Namun demikian terdapat kelemahan dimana IoT terbukti rentan terhadap pelanggaran keamanan. Oleh karena itu, perlu dikembangkan solusi dengan menciptakan teknologi baru atau menggabungkan teknologi yang sudah ada untuk mengatasi masalah keamanan. *Deep learning*, sebagai cabang *machine learning* telah menunjukkan hasil yang menjanjikan dalam penelitian sebelumnya untuk mendeteksi pelanggaran keamanan. Selain itu, perangkat IoT menghasilkan volume yang besar, variasi, dan kebenaran data. Dengan demikian, ketika teknologi *big data* dimasukkan, kinerja yang lebih tinggi dan penanganan data yang lebih baik dapat dicapai. Berbagai penelitian telah dilakukan secara komprehensif tentang *deep learning*, keamanan IoT, dan teknologi *big data*. Selanjutnya, analisis komparatif dan hubungan antara *machine learning*, keamanan IoT, dan teknologi *big data* juga telah dibahas. Taksonomi tematik dilakukan dari analisis komparatif studi teknis dari tiga domain tersebut. Penelitian ini mengidentifikasi dan mendiskusikan tantangan dalam menggabungkan *deep learning* untuk keamanan IoT menggunakan teknologi *big data* dan telah memberikan masukan berupa saran untuk penelitian yang akan datang.

Kata Kunci : Keamanan IoT, *deep learning, big data*

1. Pendahuluan

Meningkatnya penggunaan perangkat IoT mengundang para penjahat dunia maya untuk menargetkan mereka. Banyak organisasi yang menghadapi tantangan terbesar dalam pemantauan ancaman berbasis jaringan, terutama di sektor-sektor berikut: pemerintah, energi, layanan kesehatan, bank, dan pusat penelitian (Ariyaluran Habeeb, Nasaruddin, Gani, Targio Hashem, et al., 2019). Selain itu, sektor-sektor ini berinvestasi dalam alat pemantauan keamanan untuk melindungi dan mengamankan infrastruktur mereka.

Penelitian ini telah menegaskan bahwa teknologi *big data* akan mampu menangani tantangan volume, kecepatan, variasi, dan kebenaran data. Data umumnya dikategorikan sebagai *big data* berdasarkan properti yang terkait dengannya, umumnya dikenal sebagai V big data (Katal, Wazid, & Goudar, 2013). Teknologi big data adalah alat atau teknologi digunakan untuk memproses

data secara efisien. Penulis (Cárdenas et al., 2013), membahas bahwa perusahaan mengumpulkan keamanan data terkait untuk kepatuhan terhadap peraturan dan analisis forensik *post hoc*. Selanjutnya, perusahaan besar menghasilkan sekitar 10 hingga 100 miliar kegiatan per hari. Mekanisme yang ada kurang diproses pada skala besar dan analitik *big data* miliki telah digunakan untuk menganalisis dan mengkorelasikan data terkait keamanan secara efisien dan belum pernah terjadi sebelumnya.

Dalam konteks ini, penelitian ini mengusulkan untuk menggunakan *deep learning* dan teknologi *big data* untuk memperkuat keamanan perangkat IoT. Lambatnya, *machine learning* telah mendapatkan pengakuan karena fitur rekayasa non-manual, pra-pelatihan tanpa pengawasan, dan kompresi kemampuan, fitur-fitur ini membuat kemampuan kerja *deep learning* layak bahkan dalam jaringan terbatas sumber daya. Selanjutnya, *deep learning* telah diimplementasikan secara luas karena kemampuan belajar mandiri, potensi untuk menghasilkan hasil yang sangat akurat, dan waktu pemrosesan yang lebih cepat.

Tabel 1. Ringkasan literatur terbaru yang relevan dengan *machine learning*, teknologi *big data*, dan keamanan IoT

Penelitian	Tujuan/Fokus dari studi sebelumnya	Keterbatasan	Signifikansi dari penelitian	Kesenjangan Penelitian
(Hussain & Abdullah, 2018)	Survei teknologi dan teknik untuk dapat diandalkan dan aman komunikasi data	Para penulis belum membahas *big data* apa pun teknologi atau tentang *big data* secara umum	Memberikan penjelasan terperinci pada *big data*.	Teknologi Big data
(Marjani, 2017)	Menyelidiki Penelitian terkni di bidang analitik *big data* dan IoT	Tidak memiliki studi mendalam tentang IoT *Security*	Melakukan secara mendalam analisis untuk keamanan IoT.	Keamanan IoT
(Radoglou Grammatikis, Sarigiannidis, & Moscholios, 2019)	Untuk memberikan analisis keamanan IoT yang komprehensif	Diskusi tentang *deep learning* dan kurangnya diskusi tentang teknologi *big data.*	Diskusi mendalam tentang *deep learning* dan algoritmanya, serta membahas teknologi *big data*	Teknologi *Deep Learning* dan *Big Data*

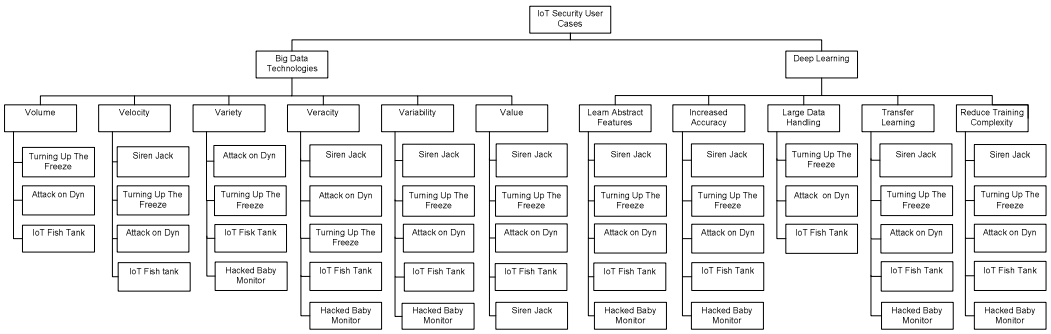
2. Kajian Pustaka

2.1. Kasus Penggunaan

Perangkat IoT telah mengalami pertumbuhan pesat dalam beberapa tahun terakhir, yang merupakan masalah besar risiko keamanan. Sampai sekarang, perangkat IoT telah terbukti memiliki kerentanan keamanan, seperti ketika perangkat IoT dikompromikan dengan *malware* Mirai dan digunakan untuk menyerang Dyn, penyedia DNS. Oleh karena itu, diperlukan teknologi baru atau kombinasi dari teknologi yang ada untuk mengamankan perangkat IoT dari penyerang. Keamanan jaringan komputer tidak terdiri dari satu aspek, tetapi mengandung empat tautan penting: perangkat lunak, perangkat keras jaringan, layanan Internet of Things dan sumber daya bersama (Munawar, Zen and Putri, 2020).

Persyaratan keamanan IoT seperti kerahasiaan, integritas, ketersediaan, otentikasi, dan kontrol membuat perangkat IoT unik dan menantang terutama bagi pengembang untuk menghasilkan sistem IoT canggih yang tahan terhadap serangan berbasis IoT. Saat banyak pengguna memanfaatkan aplikasi betbasis IoT dimana IoT menyediakan platform yang memungkinkan lembaga kesehatan masyarakat mengakses data untuk memantau pandemi COVID-19 (Komalasari, 2020), maka diperlukan keamanan IoT.

Selain itu, teknologi *big data* juga telah terbukti efektif dalam memproses berbagai jenis data. Studi seperti (Ariyaluran Habeeb, Nasaruddin, Gani, Amanullah, et al., 2019), telah menunjukkan hasil yang menjanjikan. Namun, penelitian terbatas telah dilakukan pada pemrosesan data keamanan IoT dengan teknologi *big data* dan algoritma *deep learning*. Dari hasil analisis kritis, dapat diidentifikasi bahwa hanya dua penelitian yang menggabungkan *deep learning* dan teknologi *big data* untuk keamanan IoT, yaitu (Vimalkumar & Radhika, 2017) dan (Vinayakumar, 2019). Skenario ini telah memberikan motivasi untuk melakukan penelitian ini dan penelitian ini akan memotivasi para peneliti lain di masa yang akan datang untuk menggabungkan tiga bidang yang dibahas. Gambar 1 di bawah ini mengilustrasikan kasus penggunaan keamanan IoT dengan penggantian ke teknologi *big data* dan karakteristik *deep learning*. Selain itu, kasus penggunaan telah dibahas dalam sub bagian berikut.



Gambar 1. Kasus Penggunaan Keamanan IoT

2.2 SirenJack

Kerentanan dalam sistem siaran darurat yang diproduksi oleh Acoustic Technology Inc. (ATI) diidentifikasi oleh Balint Seeber yang dijuluki SirenJack, seorang peneliti dari Bastille Security. Sistem memungkinkan siaran paket perintah melalui udara untuk ditangkap, dimodifikasi dan diputar ulang. Cacat itu ditemukan ketika Seeber mengaudit sistem peringatan darurat yang digunakan di seluruh San Francisco (Cimpanu, 2018). Kasus penggunaan SirenJack adalah jenis deteksi intrusi yang dapat dihindari menggunakan *deep learning* dan teknologi *big data* karena telah menunjukkan hasil yang menjanjikan dalam mendeteksi intrusi.

2.3 Attack on Dyn dan Tangki Ikan IoT

Serangan besar dilakukan pada Dyn, penyedia DNS terkemuka pada 21 Oktober 2016. Serangan itu adalah serangan DDoS besar yang membuat sekitar 85 situs web utama seperti Netflix, Twitter, PayPal, dan Sony PlayStation tidak responsif terhadap pengguna

Di Amerika Utara, peretas telah menggunakan tangki ikan yang terhubung ke internet untuk meretas kasino. Tangki ikan dilengkapi dengan sensor untuk mengatur suhu, pemantauan makanan, dan kebersihan tangki. Peretas menggunakan tangki ikan untuk masuk ke jaringan. Dilaporkan bahwa data bernilai 10 GB ditransmisikan ke perangkat yang berlokasi di Finlandia (Schiffer, 2017). Kasus penggunaan ini memberi bukti yang cukup bahwa perangkat IoT dapat digunakan untuk memanipulasi seluruh jaringan. Oleh karena itu, menghentikan penjahat *cybe*r di *firewall* adalah kunci untuk mencegah insiden bencana. Oleh karena itu, pemantauan berkelanjutan aliran data menggunakan teknologi *big data* dan *deep learning* akan memungkinkan deteksi pelanggaran keamanan berbasis IoT pada tahap awal.

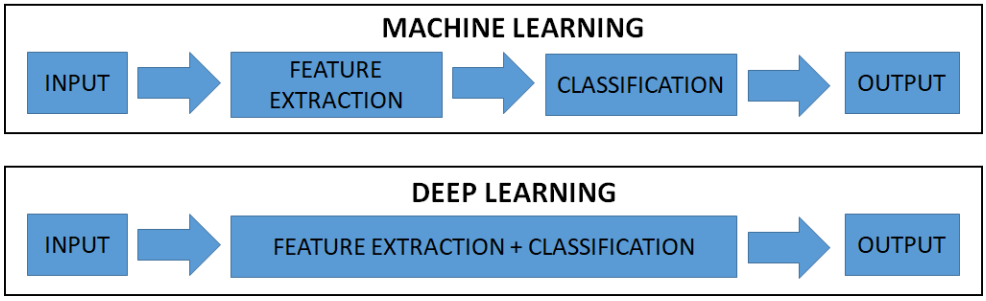
3. Analisis Big Data dan Keamanan IoT

Bagian ini berisi deskripsi yang komprehensif tentang *deep learning*, teknologi *big data*, dan keamanan IoT. Selain itu, hubungan antara ketiga domain ini telah dibahas, untuk memberikan pengetahuan dasar dan pemetaan hubungan tentang hal ini topik tersebut.

3.1. *Deep Learning*

Dalam beberapa tahun terakhir, *deep learning* telah menarik banyak peneliti dan organisasi, dibandingkan dengan pendekatan *machine learning* tradisional. Para penulis (Mohammadi, 2018) telah membandingkan empat algoritma pembelajaran mesin, seperti, *Support Vector Machine* (SVM), *Decision Trees*, K means, dan

Regresi Logistik menggunakan tren Google, dan hasilnya menunjukkan bahwa *deep learning* menjadi lebih populer. Selanjutnya, teknologi ini telah diterapkan dalam berbagai aplikasi AI seperti, pengenalan gambar, pengambilan gambar, mesin pencari dan pencarian informasi, dan pemrosesan bahasa alami. *Machine learning* dan *deep learning* memiliki empat fase dalam membangun model. Gambar 2 di bawah ini menggambarkan perbedaan antara *machine learning* dan *deep learning*.

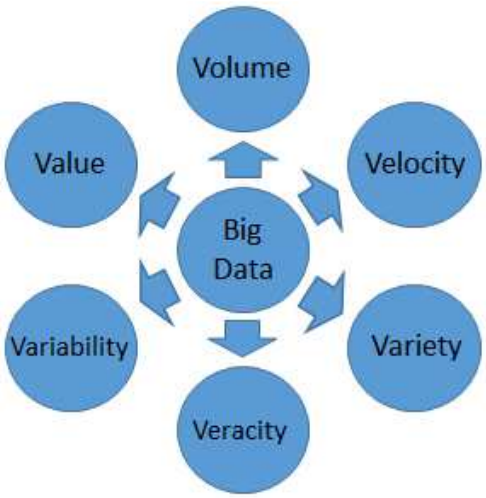


Gambar 2: Machine Learning Vs. Deep Learning

Deep learning telah mendapatkan pengakuan karena karakteristiknya yang mampu mempelajari fitur yang lebih abstrak, mengurangi kompleksitas pelatihan model, akurasi yang menjanjikan, kemampuan untuk menangani kumpulan data yang besar, dan dukungan untuk pembelajaran transfer (Guo et al., 2016).

3.2. Teknologi Big Data

Big data dapat dideskripsikan sebagai volume tinggi, kecepatan tinggi, dan variasi tinggi informasi yang menuntut bentuk inovatif dari pemrosesan informasi untuk mendapatkan wawasan dan untuk pengambilan keputusan (Gandomi & Haider, 2015). Biasanya, *big data* ditandai dengan 6 sifat, umumnya disebut sebagai 6V.



Gambar 3. 6V dari Big Data

Gambar 3 mengilustrasikan 6V, yang merupakan karakteristik dasar dari *big data*, secara umum. Data diklasifikasikan sebagai *big data* selama memenuhi 3V pertama yaitu volume, kecepatan, variasi (Adam, Fakharaldien, Zain, Majid, & Noraziah, 2019). Teknologi *big data* dapat digambarkan sebagai alat atau teknologi yang digunakan untuk memproses data secara efisien yang telah diklasifikasikan sebagai *big data*. Beberapa teknologi *big data* termasuk, Apache Hadoop (Vavilapalli, Murthy, …, & 2013, 2013), Apache Spark (Zaharia, 2016), Apache Storm (Veen, 2015), Apache Flink (Carbone, 2015), Apache Cassandra (Chebotko, 2015), dan Apache HBase (Borthakur et al., 2011). Pada gambar di atas terdapat karakteristik *big data*, yaitu 6V.

3.3 Keamanan IoT

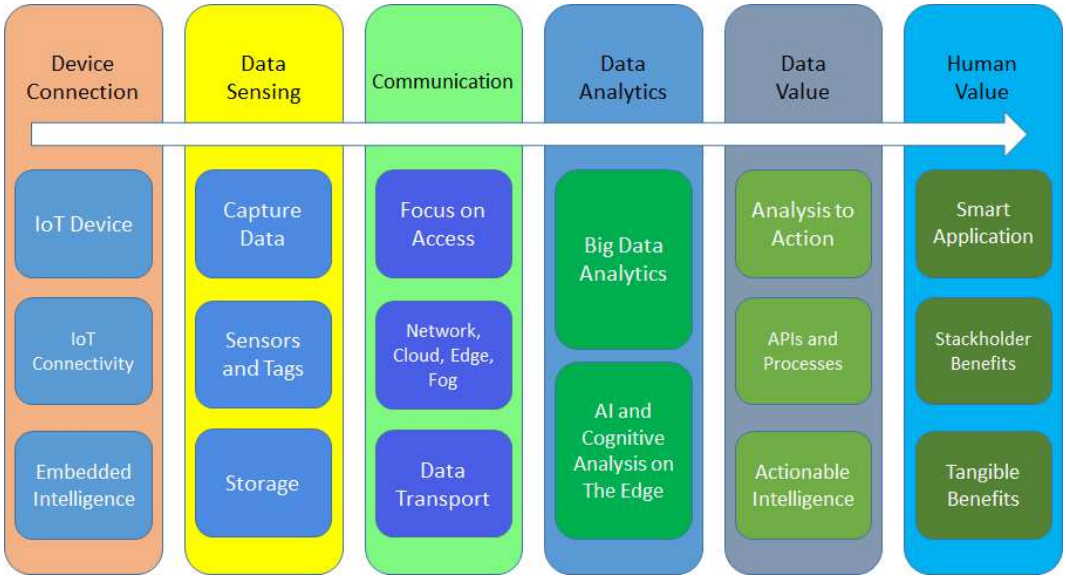
Baru-baru ini IoT telah diadopsi secara luas membangun sistem cerdas seperti, kota pintar, rumah pintar, kantor pintar, gerai ritel pintar, pertanian cerdas, pengelolaan air pintar, transportasi pintar, perawatan kesehatan pintar, dan energi pintar (Marjani, 2017). Karena penggunaan IoT yang luas dalam perangkat seluler, fasilitas transportasi, fasilitas publik, dan peralatan rumah tangga, peralatan ini dapat digunakan untuk akuisisi data di IoT. Selanjutnya, perangkat yang digunakan dalam berbagai aplikasi yang terhubung ke jaringan IoT dapat dikontrol jarak jauh. Perangkat dapat berkomunikasi satu sama lain dan juga dengan perangkat pengendali pusat. Selain itu, ketika digunakan dalam berbagai domain, berbagai data dapat dikumpulkan seperti, data geografis, astronomi, lingkungan, dan logistik [15]. Keamanan IoT dianggap sebagai pengamanan seluruh arsitektur penyebaran IoT dari serangan (Khan & Salah, 2018).

Ada berbagai faktor yang perlu dipertimbangkan untuk mengembangkan solusi keamanan IoT. Berikut ini adalah persyaratan keamanan yang harus dipenuhi untuk mengembangkan solusi keamanan IoT. Karena kemampuan luar biasa yang disediakan oleh *deep learning* dan teknologi *big data*, mereka dapat digunakan untuk mengidentifikasi kumpulan pelanggaran keamanan yang terkait dengan persyaratan keamanan.

Biasanya, teknologi *big data* terdiri dari transmisi data yang aman dengan menggunakan metodologi enkripsi, sehingga mencegah data untuk dikompromikan oleh musuh (Apark.apache.org, 2019). Integritas sistem IoT dapat dikompromikan oleh musuh. Oleh karena itu, integritas menjamin bahwa data yang diterima belum dimanipulasi selama transmisi (Khattak, Shah, Khan, Ali, & Imran, 2019).

Diketahui bahwa teknologi big data menyediakan dukungan kontrol akses untuk aplikasinya. Diperlukan filter untuk mencapai hal ini dan setiap aplikasi dapat dilengkapi dengan daftar kontrol aksesnya sendiri (Apark.apache.org, 2019). Meskipun, *deep learning* tidak secara langsung terkait dengan persyaratan keamanan IoT, pemantauan perlu dilakukan terus-menerus terhadap jaringan dan

komunikasi antara perangkat dan sistem IoT dapat membantu dalam mendeteksi dan memitigasi pelanggaran keamanan pada tahap awal. Karakteristik *deep learning* berkontribusi pada identifikasi pelanggaran keamanan, ini karena *deep learning* mampu menangani kumpulan data yang sangat besar, mengklasifikasikan data yang sah dan data anomali pada tingkat akurasi yang lebih tinggi, belajar dari data yang kompleks, dan belajar dari data dengan kecepatan yang jauh lebih cepat.



Gambar 4: Koneksi Perangkat ke Nilai Manusia di IoT

Gambar 4 mengilustrasikan koneksi ke manfaat perangkat IoT. Bagian di atas telah membahas tentang *deep learning*, teknologi *big data* dan keamanan IoT bersama dengan hubungan di antara mereka.

3.4. Taksonomi

Taksonomi ini diklasifikasikan ke dalam beberapa kategori yaitu, *deep learning*, IoT security, dan teknologi *big data*, dan selanjutnya dikategorikan sebagai arsitektur *deep learning*, kerangka kerja, evaluasi model, area aplikasi keamanan IoT, Serangan keamanan IoT, kumpulan data, apache hadoop, apache spark, dan apache storm. Karena keterbatasan penelitian yang telah dilakukan dengan menggabungkan *deep learning*, teknologi *big data*, dan keamanan IoT, kami telah mengidentifikasi hubungan di antara ketiga domain ini berdasarkan penelitian eksperimental terkait yang telah menggunakan *deep learning* dengan kombinasi antara keamanan IoT, atau teknologi *big data*, dan keamanan IoT atau teknologi *big data* dengan deteksi serangan keamanan, yang terdiri dari serangan identik seperti itu di ruang IoT.

3.5. Deep Learning

Arsitektur *deep learning* umumnya memiliki tiga jenis model pembelajaran, pembelajaran terbimbing, pembelajaran tanpa pengawasan, dan pembelajaran semi-diawasi. Dalam pembelajaran yang diawasi, data yang digunakan untuk melatih arsitektur diberi label penuh, sedangkan dalam pembelajaran yang tidak diawasi, data tidak diberi label dan arsitektur mencoba memunculkan struktur dengan mengekstraksi informasi yang berguna. Dalam model pembelajaran semi-diawasi, dataset pelatihan berisi campuran data yang berlabel dan tidak berlabel, jenis pembelajaran ini sia-sia ketika mengekstraksi fitur yang relevan dari data itu membosankan (Huang, 2014). *Deep learning* dapat dikategorikan menjadi dua jenis, diskriminatif dan generatif. Model diskriminatif umumnya mendukung metode pembelajaran terawasi, sedangkan model generatif mendukung pembelajaran tanpa metode pengawasan (Mohammadi, 2018). *Autoencoder* (AE): AE adalah jenis Jaringan Syaraf Tiruan (JST) yang mempelajari pengkodean data yang efisien dengan cara yang tidak diawasi (Liou, Huang, & Yang, 2008),. AE terdiri dari input dan lapisan output yang terhubung menggunakan satu atau lebih lapisan tersembunyi.

Tabel 2 mengklasifikasikan arsitektur yang dibahas di atas berdasarkan kategori, model pembelajaran, dan studi yang telah memanfaatkan arsitektur ini. Selain itu, hubungan dan penerapan arsitektur ini dengan teknologi *big data* dan keamanan IoT telah dibuktikan dengan membuktikan keberhasilan implementasi

Tabel 2. Arsitektur Deep Learning

Arsitektur	Kategori	Model Pembelajaran	Penelitian
AE	Generatif	Tidak diawasi	(Meidan et al., 2018)
RNN	Deskriptif	diawasi	(Thilina, 2016)
RBM	Generatif	Tidak diawasi dan diawasi	(Elsaeidy, Elgendi, Munasinghe, Sharma, & Jamalipour, 2017),
DBN	Generatif	Tidak diawasi dan diawasi	(Marir, 2018),(He, Mendis, & Wei, 2017)
LSTM	Deskriptif	Tidak diawasi	(Bipraneel, 2018),(Roopak, Yun Tian, & Chambers, 2019)
CNN	Deskriptif	Tidak diawasi	(Roopak et al., 2019),(Homayoun et al., 2019)

Keterangan :
Autoencoder (AE):
Recurrent Neural Network (RNN):
Restricted Boltzmann Machine (RBM):
Deep Belief Network (DBN):

Long Short-Term Memory (LSTM):
Convolutional Neural Network (CNN)

3.6. Keamanan IoT

Area aplikasi keamanan IoT umum di mana *deep learning* telah diterapkan secara jelas telah dibahas. Deteksi Anomali: Deteksi anomali adalah proses mengidentifikasi anomali. Anomali sering disebut sebagai pola yang tidak mengikuti pola standar. Anomali ini dihasilkan oleh aktivitas abnormal seperti, serangan dunia maya, penipuan kartu kredit, dan banyak lagi. Suatu anomali umumnya dikategorikan ke dalam tiga kategori, yaitu anomali titik, anomali kontekstual, dan anomali kolektif. Anomali titik: Jika instance data berbeda dari pola normal dalam dataset, dikatakan anomali titik. Anomali kontekstual: Jika dalam konteks tertentu, contoh data berperilaku anomali maka itu disebut anomali kontekstual. Anomali kolektif: Jika sekelompok instance data serupa berperilaku anomali dibandingkan dengan seluruh dataset, mereka dikatakan anomali kolektif (Ahmed, Naser Mahmood, & Hu, 2016).

Host Intrusion Detection System (HIDS): HIDS digunakan untuk memantau aktivitas dan karakteristik dari satu *host* di jaringan untuk aktivitas abnormal apa pun. Umumnya, agen ditempatkan ke *host* target dalam sistem deteksi intrusi berbasis *host*. Dalam beberapa kasus, agen dapat digunakan pada perangkat jarak jauh. Sensor dalam intrusi berbasis *host* sistem deteksi digunakan sebagai inline atau pasif. Dalam sensor inline, lalu lintas jaringan melewati sensor dan kemudian mencapai host target. Sensor pasif memantau replika lalu lintas jaringan nyata (Nobakht, Sivaraman, & Boreli, 2016). *Network Intrusion Detection System* (NIDS): A NIDS digunakan untuk memantau aliran lalu lintas jaringan. Lapisan jaringan yang berbeda dianalisis oleh NIDS untuk mendeteksi kemungkinan ancaman keamanan (Nobakht et al., 2016).

Deteksi *Malware*: Deteksi *malware* adalah proses mengidentifikasi malware. Biasanya, ada dua jenis deteksi malware, yaitu analisis statis atau dinamis. Dalam analisis statis, malware langsung dianalisis dalam bentuk binernya, sedangkan, dalam analisis dinamis, file biner dieksekusi dan kegiatannya dimonitor (Saxe, 2015). Deteksi *Ransomware*: Ransomware adalah sebuah tipe malware yang mengenkripsi komputer yang terkena dampak dan tebusan diminta untuk dekripsi (Kara & Aydos, 2019).

Pengguna klandestin: Seseorang yang memperoleh kontrol pengawasan sistem untuk menghindari audit dan kontrol akses atau untuk menekan pengumpulan audit (Thilina, 2016). IoT *Botnet Attack Detection*: *Bot* adalah perangkat yang terhubung ke infrastruktur protokol umum yang dikendalikan dari jarak jauh. Perangkat dapat dikompromikan dan diubah menjadi bot oleh penyerang. Ketika perangkat IoT bergabung dengan *botnet*, perangkat tersebut dapat digunakan untuk berbagai tujuan, termasuk serangan DDoS (Ceron, Steding-Jessen, Hoepers, Granville, & Margi, 2019). Deteksi serangan botnet IoT adalah tindakan

mendeteksi serangan berbasis botnet IoT seperti, DDoS. Tabel 3 menunjukkan area aplikasi keamanan IoT di mana *deep learning*, terutama dengan teknologi big data telah diterapkan.

Tabel 3. Area Aplikasi Keamanan IoT

Area Aplikasi Keamanan IoT	Penelitian
Deteksi Anomali	(Marir, 2018)
NIDS	(Bipraneel, 2018),(Dawoud, Shahristani, & Raun, 2018),(Alotaibi & Alotaibi, 2020),(Mylavarapu, 2015),(Vimalkumar & Radhika, 2017),(Vinayakumar, 2019)
Deteksi Malware	(Azmoodeh, Dehghantanha, & Choo, 2019),(HaddadPajouh, Dehghantanha, Khayami, & Choo, 2018),(Kozik, 2018)
Deteksi Ransomware	(Homayoun et al., 2019)
Deteksi Penyusup	(Thilina, 2016)
IoT Botnet Attack Detection	(Meidan et al., 2018)

Berbagai serangan keamanan IoT berdasarkan pada setiap lapisan adalah sebagai berikut. Serangan Lapisan Persepsi. Lapisan persepsi terdiri dari objek fisik seperti, sensor dan aktuator, node, dan perangkat. Serangan lapisan persepsi mempengaruhi objek fisik dalam infrastruktur IoT. Serangan lapisan persepsi umum telah diuraikan. *Botnet*: *Botnet* seperti Mirai, terdiri dari empat komponen utama: *bot* adalah malware yang menginfeksi perangkat.

SYN *Flood*: Dalam serangan SYN *Flood* penyerang mengirimkan sejumlah besar paket SYN *Transmission Control Protocol* (TCP) ke target. Ini memaksa target untuk menggunakan sumber daya terbatas seperti, CPU, *bandwidth*, dan memori untuk membalas SYN(Bijalwan, 2015). Kecepatan serangan yang tinggi akan menyebabkan serangan DoS dan akhirnya tidak dapat melayani pengguna asli (Beaumont-Gay, 2007). *Ping of Death*: *Ping of Death* adalah serangan, di mana penyerang mengirimkan ping berukuran sangat besar ke target dengan maksud untuk menjatuhkan target.

Routing Attacks: Dalam serangan routing, node berbahaya meluncurkan jenis serangan routing untuk mengganggu operasi routing atau untuk melakukan serangan DoS (Kannhavong, Nakayama, Nemoto, Kato, & Jamalipour, 2007). *Sybil Attact*: Selama serangan Sybil, node jahat merusak sistem perutean, dan mengakses informasi yang diblokir oleh node, atau jaringan dipartisi. Serangan ini dieksekusi oleh penyerang tunggal yang menciptakan banyak identitas palsu dan berpura-pura menjadi banyak dalam jaringan *peer-to-peer* (P-2-P) (Trifa & Khemakhem, 2014).

Middleware Attact: Dalam infrastruktur IoT middleware terdiri dari komponen-komponen seperti cloud. Serangan middleware secara langsung melibatkan aktivitas jahat pada komponen middleware dari infrastruktur IoT. *Cloud Based*: Dalam serangan *cloud based*, penyerang langsung menyerang platform *cloud* karena berbagai alasan, seperti pencurian informasi, *flood attact*, dan sebagainya. Serangan berbasis cloud yang umum adalah : *Cloud Malware Injection*: Selama serangan injeksi *malware cloud*, seorang penyerang mendapatkan akses ke data korban di *cloud* dan mengunggah salinan jahat dari *instance* layanan korban, oleh karena itu memungkinkan layanan korban diproses dalam *instance* berbahaya (Gruschka & Jensen, 2010). *Cloud Flooding Attack*: Serangan *cloud flooding* memungkinkan penyerang mengirim sejumlah besar paket dari *host* yang tidak bersalah dalam jaringan untuk membanjiri korban. Paket besar ini dapat berupa kombinasi atau banyak TCP, UDP, dan ICMP. Selanjutnya, jenis serangan ini dapat mempengaruhi kemampuan layanan untuk melayani pengguna yang berwenang. Selain itu, penggunaan cloud dapat meningkat karena tidak memiliki kemampuan mengidentifikasi lalu lintas yang sah dan menyerang (Modi et al., 2013).

Serangan Otentikasi: Serangan berbasis otentikasi digunakan untuk mengeksploitasi proses otentikasi yang digunakan untuk memverifikasi pengguna, layanan, atau aplikasi (Liu, Xiao, & Chen, 2012). *Brute Force*: Serangan brute-force membuat penyerang mendapatkan akses dengan memasukkan berbagai kredensial login dengan harapan menebak kredensial dengan benar. Penyerang memasuki berbagai kemungkinan kata sandi sampai kata sandi yang tepat ditemukan (Herley & Florêncio, 2008). Dictionary Attack: Serangan kamus juga disebut sebagai serangan mempertanyakan kata sandi adalah ketika seorang penyerang telah membangun database dengan kemungkinan kata sandi. Penyerang mengeksekusi ini dengan menguping di saluran dan mencatat transkrip. Setelah itu, kata sandi dicoba untuk dibuat agar sesuai dengan yang direkam. Jika kecocokan telah ditemukan, maka penyerang telah berhasil memperoleh kata sandi (Chakrabarti & Singhal, 2007). *Reply Attact*: Serangan *replay* memungkinkan penyerang mencegat dan menangkap komunikasi atau tindakan digital dan menggunakannya pada titik waktu berikutnya. memungkinkan penyerang menggunakan informasi orang lain untuk menyamar sebagai orang itu (Smith, Wiliem, & Lovell, 2015). *Signature Wrapping Attact* : *Signature wrapping attact* memungkinkan penyerang muncul sebagai pengguna yang sah dan melakukan permintaan layanan web sewenang-wenang. Ini dicapai dengan menyuntikkan elemen jahat ke dalam struktur pesan, ini memastikan tanda tangan yang valid untuk elemen yang sah dan pemrosesan elemen jahat dalam logika aplikasi (Gajek, Jensen, Liao, & Schwenk, 2009).

Code Injection Attact: Serangan injeksi kode berfokus pada mendepositkan kode yang dapat dieksekusi berbahaya (kode mesin) ke ruang alamat dari proses korban, dan kemudian memberi wewenang kontrol ke kode ini (Kc, 2003). *Structured Query Language* (SQL) *Injection*: SQL *injectio* dijalankan melalui *statement* SQL *database* berbahaya dengan mengambil keuntungan dari validasi

aliran data dari pengguna ke *database* (Kiezun, Guo, Jayaraman, & Ernst, 2009). Injeksi Skrip: Selama injeksi skrip atau *Cross-Site Scripting* (XSS), skrip jahat, yang umumnya ditulis dalam JavaScript disuntikkan ke dalam konten situs web. Skrip berbahaya mampu membocorkan informasi sensitif dari situs (Jim, Swamy, & Hicks, 2007). *Injeksi Shell:* Serangan injeksi shell kadang-kadang disebut sebagai serangan injeksi perintah menyuntikkan perintah jahat ke dalam sistem untuk melakukan aktivitas jahat (Gao, Morris, Reaves, & Richey, 2010).

Tabel 4 merinci beberapa serangan penting pada ruang IoT untuk setiap lapisan. *Dataset* yang sering digunakan untuk analisis eksperimental pada *deep learning*, teknologi *big data* dan / atau untuk keamanan IoT atau keamanan jaringan adalah sebagai berikut. UNSW-NB15: *Dataset* UNSW-NB15 dikembangkan pada tahun 2015, yang terdiri dari kombinasi data serangan normal yang disintesis normal *modern* dan kontemporer. Ini adalah *dataset* berlabel dan terdiri dari total 47 fitur. Selanjutnya, *dataset* ini terdiri dari 9 tipe serangan, yaitu fuzzes, analisis, *backdoors*, DoS, *exploit*, *generic*, *reconnaissance shellcode*, dan jenis serangan worm (Moustafa, Slay, & Technology, 2015).

Tabel 4. Serangan Terkemuka di IoT

Menyerang Lapisan	Tipe Penyerang	Tahun	Judul	Deskripsi	Hasil / Dampak	Sitasi
Fisik	Botnet	2012	Carna Botnet	Digunakan untuk mengukur luasnya network	Ditemukan 1,3 miliar IPv4 alamat sedang digunakan, di mana 141 juta berada di belakang firewall dan 729 juta membalikkan catatan DNS. Tersisa 2,3 miliar IPv4 alamat tidak digunakan	(J. Horchert, 2013) (Kleinman, 2017)
Jaringan	Domain Name System hijacking	2017	-	Domain Name System hijacking menyerang pemerintah agensi, telekomunikasi perusahaan, dan raksasa internet di 13 negara selama 2 tahun	Perbarui catatan DNS organisasi begitu informasinya akan dialihkan ke peretas yang ditentukan server	(Avast Security News Team, 2019)

NSL-KDD: *Dataset* ini merupakan perpanjangan dari *dataset* KDDCUP99, di mana catatan yang dipilih diekstraksi dari seluruh dataset KDDCUP99. Dalam penelitian (Tavallaee, Bagheri, Lu, & Ghorbani, 2009), *dataset* KDDCUP99 sangat mempengaruhi kinerja sistem yang dievaluasi dan menghasilkan buruknya evaluasi teknik deteksi anomali. Karena itu, telah diusulkan NSL-KDD, yang tidak termasuk catatan redundan di set kereta, set tes yang diusulkan tidak mengandung catatan duplikat, di tangan di setiap tingkat kesulitan jumlah catatan yang dipilih berbanding terbalik dengan persentase catatan dalam dataset KDDCUP99 , dibuat oleh penulis studi (Stolfo, Fan, Lee, Prodromidis, & Chan, 2000) berdasarkan pada program evaluasi IDS DARPA'98 (Lippmann et al., 2000).

3.7. Teknologi Big Data

Subbagian ini membahas teknologi big data penting yang ada yang diterapkan dalam konteks *deep learning* untuk keamanan IoT atau keamanan jaringan. Selain itu, teknologi big data, platform pengembangan mereka, versi stabil terbaru, tanggal rilis stabil terbaru, dan beberapa studi yang telah menerapkan teknologi big data dengan *deep learning* dan / atau untuk keamanan IoT atau keamanan jaringan.

Apache Hadoop adalah alat pemrosesan batch yang menyediakan skalabilitas dan toleransi kesalahan. Hadoop mendukung petabyte data dan memungkinkan aplikasi dijalankan pada banyak node. Selain itu, data log dipecah menjadi blok dan dikirim ke node di Hadoop gugus. Selain itu, Hadoop populer karena kemampuan pengambilan cepat, pencarian data log, skalabilitas, penyisipan data yang lebih cepat, dan toleransi kesalahan (Mavridis & Karatza, 2017).

Apache Spark dikembangkan sebagai model terpadu untuk pemrosesan data terdistribusi oleh University of California, Berkely pada tahun 2009. Spark memperluas model MapReduce dengan abstraksi berbagi data yang disebut Resilient Distributed Dataset (RDD). Menggunakan ekstensi ini, Spark dapat menangkap dan memproses beban kerja seperti, SQL, streaming, pembelajaran mesin, dan pemrosesan grafik (Zaharia, 2016).

Apache Storm adalah sistem perhitungan real-time open source. Storm memungkinkan pemrosesan aliran data secara praktis. Lebih lanjut, ia mampu memproses jutaan tupel per detik per node. Storm cepat, scalable, toleran terhadap kesalahan, dan ramah pengguna. Bahkan, storm menyediakan kemampuan untuk menggabungkan basis data dalam pemrosesan (Veen, 2015).

3.8. Deep Learning untuk Keamanan IoT menggunakan Teknologi Big Data

Bagian ini terdiri wawasan teknik canggih dalam kasus di mana *deep learning* telah diterapkan untuk keamanan IoT, penerapan *deep learning* bersama dengan teknologi *big data*. Akhirnya, tinjauan komprehensif *deep learning*, *data* dan keamanan IoT telah disajikan.

3.9. Deep Learning dan Keamanan IoT

Pada bagian ini membahas teknik canggih yang digunakan untuk keamanan IoT menggunakan teknik *deep learning*. IoT telah mendapatkan banyak perhatian sehingga militer pun menggunakan IoT. Internet of Battlefield Things (IoBT) disebut sebagai penggunaan IoT untuk operasi militer dan aplikasi pertahanan. Para penulis penelitian (Azmoodeh et al., 2019) telah mengidentifikasi bahwa injeksi malware adalah serangan yang paling umum. Selanjutnya, mereka telah mengusulkan Eigenspace yang mendalam pendekatan pembelajaran untuk mendeteksi malware IoBT melalui urutan Operational Codes (OpCode) perangkat. OpCodes ditransmutasikan ke dalam ruang vektor dan pembelajaran Eigenspace yang mendalam.

Ransomware, adalah malware yang berkembang pesat yang telah mempengaruhi berbagai industri di berbagai negara. Oleh karena itu, studi (Homayoun et al., 2019) mengusulkan model yang menggunakan LSTM dan CNN untuk membedakan ransomware dan goodware dalam jaringan. Metrik evaluasi yang digunakan untuk model adalah f-ukur, TPR, FPR, dan MCC.
Tabel 5 membahas tentang area aplikasi, algoritma *deep learning*, batasan studi dan kutipan dari keadaan seni yang dibahas untuk *deep learning* dan keamanan IoT.

Tabel 5. Deep Learning dan Keamanan IoT

Area Aplikasi	Arsitektur Deep Learning / model	Keterbatasan Studi	Sitasi
Deteksi Malware	Jaringan konvolusional	Dataset yang dibuat sendiri. Sampel malware terbatas dalam dataset.	(Azmoodeh et al., 2019)
Deteksi Serangan botnet IoT	DAE	Model hanya dievaluasi pada Mirai dan botnet BASHLITE. Model yang	(Meidan et al., 2018)

		diusulkan dibandingkan dengan 3 pembelajaran mesin algoritma.	

3.10. Deep Learning dan Teknologi Big Data

Pada penelitian (Gupta, Thakur, Shrivastava, Kumar, & Nag, 2017) miliki mengusulkan kerangka kerja yang menggabungkan Apache Spark dan Multi-Layer Perceptron (MLP) menggunakan pembelajaran kaskade. Kerangka kerja terdiri dari tiga tahap, tahap pertama adalah input dataset ke dalam Apache Spark, tahap kedua adalah metode pembelajaran kaskade, dan yang ketiga algoritma deep stage learning diterapkan. Kerangka kerja tersebut telah dievaluasi berdasarkan dua metrik, skor f1 dan akurasi. Mereka telah mengklaim bahwa mereka telah dapat memperoleh model yang melakukan analisis *big data* skala besar dalam waktu singkat, dengan lebih sedikit kompleksitas komputasi dan dengan akurasi yang lebih tinggi secara signifikan. Tak perlu dikatakan, keakuratannya dan skor f1 dari model yang diusulkan tidak mencapai bahkan 75% untuk semua tahap. Selanjutnya, teknologi big data terbatas telah dimasukkan ke dalam kerangka kerja yang diusulkan. Selain itu, dalam penelitian (Marir, 2018) penulis telah sangat mengklaim bahwa teknik pembelajaran mesin tidak cukup kuat untuk mendeteksi serangan canggih di IDS yang ada. Karena itu, mereka punya mengusulkan pendekatan terdistribusi untuk deteksi perilaku abnormal dalam jaringan skala besar.

Pada penelitian (Khumoyun, Cui, & Hanku, 2016) telah merancang dan menerapkan kerangka kerja yang melatih DNN menggunakan Apache Spark. Pelatihan model *deep learning* membutuhkan yang besar jumlah data dan luas komputasi. Mereka telah mengklaim bahwa Kerangka kerja dapat mempercepat waktu pelatihan dengan mendistribusikan replika model, melalui keturunan gradien stokastik, di antara node untuk data dalam Sistem File Terdistribusi Hadoop (HDFS). Kerangka kerja tersebut dievaluasi berdasarkan run time, akurasi, dan tingkat kesalahan. Itu Kerangka yang diusulkan telah menunjukkan kinerja waktu dan akurasi yang memuaskan. Sebaliknya, waktu menjalankan model menunjukkan peningkatan ketika jumlah node lebih sedikit. Bahkan, terlihat bahwa tingkat kesalahan berkurang hanya ketika jumlah iterasi meningkat.

3.11. Deep Learning dan Teknologi big data untuk keamanan IoT

Berdasarkan analisi, telah berupaya mengatasi hubungan antara *deep learning*, *big data*, dan keamanan IoT. Namun, penelitian sebelumnya hanya dimasukkan baik *deep learning* dan keamanan IoT atau *deep learning* dan teknologi *big data*. Selanjutnya, penelitian telah dilakukan pada *deep learning*, teknologi *big data*, dan keamanan IoT. Selain itu, dengan upaya maksimal untuk menganalisis

berbagai peneltian secara kritis, telah mampu mengidentifikasi hanya dua studi yang telah membahas ketiga komponen tersebut. Kelebihan dan kekurangan dari kedua studi telah dijelaskan. Karena pertumbuhan eksponensial dari berbagai perangkat yang saling berhubungan, serangan inovatif terjadi dan sedang dilakukan pada perangkat ini. Karena itu, perlu upaya inovatif dan metodologi untuk mencegah insiden bencana. Oleh karena itu, penulis [29] merancang kerangka *big data* untuk deteksi intrusi menggunakan metode klasifikasi seperti, DNN, SVM, *random forest*, pohon keputusan, dan Bayes naif. Metrik yang digunakan untuk evaluasi serta akurasi, daya ingat, *false degre*, spesifisitas, dan waktu prediksi.

Apache Spark telah digunakan sebagai platform untuk menerapkan deteksi intrusi di smart grid menggunakan analitik *big data*. Mereka mengklaim bahwa algoritma DNN mendapatkan akurasi tertinggi untuk dataset mentah. Meskipun demikian, akurasi tertinggi yang diperoleh adalah oleh model DNN, tetapi akurasinya kurang dari 80%. Selain itu, waktu prediksi DNN lebih tinggi dibandingkan dengan model lain. Selain itu, penulis dalam penelitian ini [30] telah membahas kemajuan dalam perangkat keras, perangkat lunak, dan topologi jaringan, termasuk IoT, hal yang menimbulkan ancaman keamanan yang memerlukan modern pendekatan yang akan diterapkan. Dengan demikian, mereka mengusulkan IDS berbasis DNN. Itu DNN yang digunakan adalah MLP bersama dengan FFNN. Telah dibahas bahwa kerangka kerjanya telah dikembangkan berdasarkan teknologi *big data*, *platform* komputasi cluster Apache Spark. Komputasi cluster spark Apache adalah setup melalui Apache Hadoop Yet Another Resource Negosiator. Telah mengevaluasi model berdasarkan akurasi, presisi, daya ingat, f-score, TPR, dan FPR. Selain itu, model mereka telah mengungguli semua mesin tradisional lainnya pendekatan pembelajaran di HIDS dan NIDS. Namun, dalam kalsifikasi multi-kelas akurasi turun di bawah 90% untuk serangan tertentu di beberapa dataset. Selanjutnya, DNN tidak dilatih tentang dataset patokan IDS.

Tabel 6. Kajian Deep Learning, Teknologi Big Data dan Keamanan IoT

Studi	Deep Learning	Teknologi Big Data	Keamanan IoT
(Mylavarapu, 2015)	✓	✓	
(Thilina, 2016)	✓	✓	
(Hsieh & Chan, 2016)	✓	✓	
(Gupta et al., 2017)	✓	✓	
(Meidan et al., 2018)	✓		✓

Seperti yang terlihat dari Tabel 6, hanya *deep learning* dan keamanan IoT atau *deep learning* dan teknologi *big data* telah dimasukkan dalam penelitian ini. Keberhasilan implementasi studi (Vimalkumar & Radhika, 2017) dan

(Vinayakumar, 2019), meyakinkan para peneliti bahwa *deep learning* dan teknologi *big data* dapat digabungkan untuk keamanan IoT. Karena itu, karena terbatasnya penelitian yang dilakukan pada bidang-bidang ini, dianjurkan untuk peneliti masa yang akan datang untuk mengimplementasikan model berdasarkan berbagai algoritma *deep learning*, dan teknologi *big data* untuk keamanan IoT.

3.12. Infrastruktur cloud untuk deep learning, teknologi big data, dan keamanan IoT

Subbagian ini merinci infrastruktur cloud yang dapat diterapkan untuk *deep learning*, teknologi *big data*, dan keamanan IoT. *Deep learning* telah menunjukkan hasil yang menjanjikan di banyak domain, namun *deep learning* mungkin cukup komputasional dalam skala besar aplikasi. Pada gilirannya, masuknya sumber daya komputasi tambahan. Kapan *deep learning* diterapkan pada aplikasi skala besar, sumber daya yang ada mungkin terbatas. Oleh karena itu, infrastruktur *cloud* dapat digunakan untuk mengatasi tantangan ini karena mengandung banyak jumlah sumber daya seperti, CPU *multi-core*, GPU *multi-core*, memori, dan *bandwidth*. Selain itu, beberapa infrastruktur *cloud* bahkan menyediakan dukungan untuk teknologi *big data* dan IoT.
Telah mentabulasi beberapa layanan *cloud* populer dan dukungan mereka untuk *deep learning* , teknologi *big data* dan IoT pada Tabel 8.

Tabel 7. Infrastruktur cloud untuk Deep Learning, Teknologi Big Data dan IoT

Layanan Cloud	Mendukung Deep Learning	Mendukung Teknologi Big Data	Mendukung IoT
Google Cloud	✓	✓	✓
AWS Sagemaker	✓	✓	✓
Deep Cognition	✓	✓	✓
IBM Watson	✓	✓	✓
Microsoft Azure	✓	✓	✓
Oracle Cloud	✓	✓	✓
Alibaba Cloud	✓	✓	✓
Tensor Pad	✓	-	-

Kemungkinan *cloud* yang berkembang dan berkontribusi pada pertumbuhan *Crimeware-as-a-Service* (CaaS), yang memungkinkan penjahat *cyber* dengan keahlian teknis terbatas untuk melakukan serangan terorganisir dan otomatis (Sood, 2013). Ada banyak jenis layanan yang disediakan oleh CaaS seperti, layanan broker bayangan, kit eksploitasi Neutrino, perangkat Mirai untuk disewakan, DiamondFox layanan malware modular.

3.12. Tantangan terbuka dan arah masa depan

Bagian ini menyoroti tantangan penelitian yang paling signifikan dalam hal keamanan IoT menggunakan *deep learning* bdan teknologi *big data*. Kemampuan canggih di IoT keamanan, *deep learning*, dan teknologi *big data* telah diperiksa untuk menentukan tantangan penelitian utama, saran, dan arah masa depan.

3.13. Deteksi ancaman keamanan

Karena kecepatan tinggi dan variasi dalam beberapa aplikasi IoT domain, struktur yang kompleks data membuatnya lebih menantang untuk mendeteksi ancaman keamanan. Selanjutnya, memilih serangkaian fitur yang diakui untuk analitik keamanan dalam algoritma *deep learning*(Rav, Wong, Lo, & Yang, 2017). Mekanisme yang ada kurang efisien dalam menemukan korelasi tersembunyi di antara fitur ini. Lebih lanjut, algoritma *deep learning* yang muncul dapat menangani parameter tersembunyi dari aplikasi IOT. Selain itu, *deep learning* mampu menemukan korelasinya dalam berbagai data. Selain itu, dimungkinkan untuk memperoleh tingkat deteksi tinggi untuk dideteksi serangan zero-day lebih efisien (Tang, Mhamdi, McLernon, Zaidi, & Ghogho, 2016). Terakhir, dibandingkan dengan pendekatan tradisional, distribusi representasi dari algoritma *deep learning* dapat menangani pemilihan banyak fitur dengan data yang luar biasa untuk mengekstrak informasi untuk aplikasi IoT multi-domain (Wang, 2017).

3.14. Komputasi dalam memori, keterbatasan komputasi dan energy

Pemrosesan dalam memori adalah teknologi pengembangan yang sedang tren untuk memproses data disimpan dalam basis data dalam memori. Ini memainkan peran penting dalam analitik streaming dan *memory centric* Arsitektur. Teknik konvensional didasarkan pada penyimpanan disk dan relasional database yang menghadapi banyak tantangan untuk menangani volume data modern dari perangkat IoT. Data yang disimpan dengan cepat diakses ketika disimpan dalam RAM atau memori *flash* dibandingkan dengan penyimpanan *disk*. Selanjutnya, memori pemrosesan memungkinkan data dianalisis secara *real time*. Pemrosesan *real-time* membantu membuat pelaporan dan pengambilan keputusan yang lebih cepat untuk ancaman keamanan. Teknologi *big data* modern seperti *Apache Spark* dan *Apache Flink* memproses data mereka dalam memori. Menggabungkan ini teknologi untuk mengembangkan analitik keamanan baru akan meningkatkan kinerja dan efisiensi untuk analitik keamanan (Ariyaluran Habeeb, Nasaruddin, Gani, Targio Hashem, et al., 2019).

Kompleksitas komputasi adalah salah satu tantangan penelitian terpenting dalam bidang keamanan perangkat IoT, *deep learning*, dan *big data*. Perangkat IoT dioperasikan di baterai berdaya rendah dan CPU-nya memiliki tingkat clock yang lebih rendah. Melakukan perhitungan apa pun dalam perangkat IoT harus cepat dan harus meminimalkan operasi langsung (Hossain, 2015).

4. Kesimpulan

Perkembangan yang pesat dari perangkat IoT telah berkontribusi pada pertimbangan keamanan risiko yang terkait. Perangkat IoT terbukti rentan karena baru-baru ini adanya peningkatan serangan seperti, *botna Carna* dan *Mirai*. Selain itu, perangkat IoT menghasilkan volume besar, kecepatan dan variasi data. Ini membuat solusi yang ada kurang efisien dan membutuhkan solusi *modern*. Dalam hal ini, *deep learning* telah diterima secara luas di kalangan peneliti dan organisasi karena akurasi tinggi, kemampuan untuk mempelajari fitur mendalam, dan pengawasan manusia yang minimal. Selain itu, teknologi *big data* juga menarik karena kemampuan mereka dalam memproses sejumlah besar data, bersama dengan kemampuan mereka untuk memproses data dalam berbagai lingkungan seperti kumpulan *real-time*. Hasil penelitian menyelidiki kemungkinan memasukkan teknologi *deep learning* dan *big data* untuk keamanan IoT. Temuan kami menunjukkan bahwa banyak penelitian telah tergabung dengan keamanan IoT atau *deep learning* dengan teknologi *big data*, namun, demikian terdapat kekurangan penelitian dalam menggabungkan teknologi *deep learning* dan *big data* untuk keamanan IoT. Terdapat dua penelitian telah membuktikan efisiensi dan kelayakan menggabungkan *deep learning* dan teknologi *big data* untuk keamanan IoT berakhir model tradisional. Perlunya mempertimbangkan berbagai persyaratan keamanan IoT yang dibahas dan tantangan yang dibahas. Kerangka kerja untuk keamanan IoT berdasarkan *deep learning* dan *big data* dan kinerja analisis eksperimental untuk membuktikan keampuhannya, dalam waktu dekat.

Daftar Pustaka

Adam, K., Fakharaldien, M. A. I., Zain, J. M., Majid, M. A., & Noraziah, A. (2019). BigData: Issues, Challenges, Technologies and Methods. *Lecture Notes in Electrical Engineering*, *520*(April), 541–550. https://doi.org/10.1007/978-981-13-1799-6_56

Ahmed, M., Naser Mahmood, A., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, *60*, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

Alotaibi, B., & Alotaibi, M. (2020). A Stacked Deep Learning Approach for IoT Cyberattack Detection. *Journal of Sensors*, *2020*. https://doi.org/10.1155/2020/8828591

Apark.apache.org. (2019). Spark Security. Retrieved October 12, 2020, from https://spark.apache.org/docs/latest/security.html

Ariyaluran Habeeb, R. A., Nasaruddin, F., Gani, A., Amanullah, M. A., Abaker Targio Hashem, I., Ahmed, E., & Imran, M. (2019). Clustering-based real-time anomaly detection—A breakthrough in big data technologies. *Transactions on Emerging Telecommunications Technologies*, (January), 1–27. https://doi.org/10.1002/ett.3647

Ariyaluran Habeeb, R. A., Nasaruddin, F., Gani, A., Targio Hashem, I. A., Ahmed, E., & Imran, M. (2019). Real-time big data processing for anomaly detection: A Survey. *International Journal of Information Management*,

45(August), 289–307. https://doi.org/10.1016/j.ijinfomgt.2018.08.006

Avast Security News Team. (2019). Sea turtle dns hijacking and more weekly news. Retrieved from https://blog.avast.com/sea-turtle-dns-hijacking

Azmoodeh, A., Dehghantanha, A., & Choo, K. K. R. (2019). Robust Malware Detection for Internet of (Battlefield) Things Devices Using Deep Eigenspace Learning. *IEEE Transactions on Sustainable Computing*, *4*(1), 88–95. https://doi.org/10.1109/TSUSC.2018.2809665

Beaumont-Gay, M. (2007). A Comparison of Syn Flood Detection Algorithms. *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, 9. https://doi.org/10.1109/icimp.2007.1

Bijalwan, A. (2015). Forensics of Random-udp Flooding Attacks. *Journal of Networks*, *10*(5), 287. https://doi.org/10.4304/jnw.10.5.287-293

Bipraneel, R. (2018). A Deep Learning Approach for Intrusion Detection in Internet of Things using Bi-directional Long Short-Term Memory Recurrent Neural Network. *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, 1–6.

Borthakur, D., Gray, J., Sarma, J. Sen, Muthukkaruppan, K., Spiegelberg, N., Kuang, H., … Aiyer, A. (2011). Apache hadoop goes realtime at Facebook. *Proceedings of the ACM SIGMOD International Conference on Management of Data*, 1071–1080. https://doi.org/10.1145/1989323.1989438

Carbone, P. (2015). Apache Flink—: Stream and Batch Processing in a Single Engine. *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering*, *36*, 4.

Cárdenas, A. A., Mcdaniel, P., Smith, S. W., Manadhata, P. K., Hp, |, Sreeranga, L., & Rajan, P. (2013). *Big Data Analytics for Security*. (December), 74–76.

Ceron, J. M., Steding-Jessen, K., Hoepers, C., Granville, L. Z., & Margi, C. B. (2019). Improving iot botnet investigation using an adaptive network layer. *Sensors (Switzerland)*, *19*(3), 1–16. https://doi.org/10.3390/s19030727

Chakrabarti, S., & Singhal, M. (2007). *Preventing Offline Dictionary Attacks*. *40*(6), 68–74. https://doi.org/10.1109/mc.2007.216

Chebotko, A. (2015). A Big Data Modeling Methodology for Apache Cassandra. *IEEE International Congress on Big Data*, 238–245. IEEE.

Cimpanu, C. (2018). SirenJack Attack Lets Hackers Take Control Over Emergency Alert Sirens. Retrieved September 19, 2020, from https://www.bleepingcomputer.com/news/security/sirenjack-attack-lets-hackers-take-control-over-emergency-alert-sirens/

Dawoud, A., Shahristani, S., & Raun, C. (2018). Deep learning and software-defined networks: Towards secure IoT architecture. *Internet of Things*, *3–4*, 82–89. https://doi.org/10.1016/j.iot.2018.09.003

Elsaeidy, A., Elgendi, I., Munasinghe, K. S., Sharma, D., & Jamalipour, A. (2017). A smart city cyber security platform for narrowband networks. *2017 27th International Telecommunication Networks and Applications Conference, ITNAC 2017*, *2017-Janua*, 1–6. https://doi.org/10.1109/ATNAC.2017.8215388

Gajek, S., Jensen, M., Liao, L., & Schwenk, J. (2009). Analysis of signature wrapping attacks and countermeasures. *2009 IEEE International Conference*

on Web Services, ICWS 2009, 575–582. https://doi.org/10.1109/ICWS.2009.12

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, *35*(2), 137–144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Gao, W., Morris, T., Reaves, B., & Richey, D. (2010). On SCADA control system command and response injection and intrusion detection. *General Members Meeting and ECrime Researchers Summit, ECrime 2010*, 1–9. https://doi.org/10.1109/ecrime.2010.5706699

Gruschka, N., & Jensen, M. (2010). Attack surfaces: A taxonomy for attacks on cloud services. *Proceedings - 2010 IEEE 3rd International Conference on Cloud Computing, CLOUD 2010*, 276–279. https://doi.org/10.1109/CLOUD.2010.23

Guo, Y., Liu, Y., Oerlemans, A., Lao, S., Wu, S., & Lew, M. S. (2016). Deep learning for visual understanding: A review. *Neurocomputing*, *187*, 27–48. https://doi.org/10.1016/j.neucom.2015.09.116

Gupta, A., Thakur, H. K., Shrivastava, R., Kumar, P., & Nag, S. (2017). A Big Data Analysis Framework Using Apache Spark and Deep Learning. *IEEE International Conference on Data Mining Workshops, ICDMW*, *2017-Novem*(1), 9–16. https://doi.org/10.1109/ICDMW.2017.9

HaddadPajouh, H., Dehghantanha, A., Khayami, R., & Choo, K. K. R. (2018). A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting. *Future Generation Computer Systems*, *85*, 88–96. https://doi.org/10.1016/j.future.2018.03.007

He, Y., Mendis, G. J., & Wei, J. (2017). Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism. *IEEE Transactions on Smart Grid*, *8*(5), 2505–2516. https://doi.org/10.1109/TSG.2017.2703842

Herley, C., & Florêncio, D. (2008). Protecting financial institutions from brute-force attacks. *IFIP International Federation for Information Processing*, *278*, 681–685. https://doi.org/10.1007/978-0-387-09699-5_45

Homayoun, S., Dehghantanha, A., Ahmadzadeh, M., Hashemi, S., Khayami, R., Choo, K. K. R., & Newton, D. E. (2019). DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer. *Future Generation Computer Systems*, *90*, 94–104. https://doi.org/10.1016/j.future.2018.07.045

Hossain, M. M. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in The Internet of Things. *015 IEEE World Congress on Services*, 21–28.

Hsieh, C. J., & Chan, T. Y. (2016). Detection DDoS attacks based on neural-network using Apache Spark. *2016 International Conference on Applied System Innovation, IEEE ICASI 2016*, 1–4. https://doi.org/10.1109/ICASI.2016.7539833

Huang, G. (2014). Semi-Supervised and Unsupervised Extreme Learning Machines. *IEEE Transactions on Cybernetics*, *4*(12), 2405–2417.

Hussain, R., & Abdullah, I. (2018). Review of Different Encryptionand Decryption Techniques Used for Security and Privacy of IoT in Different

Applications. *2018 6th IEEE International Conference on Smart Energy Grid Engineering, SEGE 2018*, 293–297. https://doi.org/10.1109/SEGE.2018.8499430

J. Horchert. (2013). Mapping the internet: A hacker's secret internet census - spiegel online - international. Retrieved from https://www.spiegel.de/international/world/hacker-measures-the-internet-illegally-with-carna-botnet-a-890413.html

Jim, T., Swamy, N., & Hicks, M. (2007). Defeating script injection attacks with browser-enforced embedded policies. *16th International World Wide Web Conference, WWW2007*, 601–610. https://doi.org/10.1145/1242572.1242654

Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., & Jamalipour, A. (2007). A survey of routing attacks in mobile ad hoc networks. *IEEE Wireless Communications*, *14*(5), 85–91. https://doi.org/10.1109/MWC.2007.4396947

Kara, I., & Aydos, M. (2019). Static and Dynamic Analysis of Third Generation Cerber Ransomware. *International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, IBIGDELFT 2018 - Proceedings*, 12–17. https://doi.org/10.1109/IBIGDELFT.2018.8625353

Katal, A., Wazid, M., & Goudar, R. H. (2013). Big Data: Issues, Challenges, Tools and Good Practices. *2013 6th International Conference on Contemporary Computing, IC3 2013*, 404–409. https://doi.org/10.1109/IC3.2013.6612229

Kc, G. S. (2003). Countering Code-Injection Attacks With Instruction-Set Randomization. *Proceedings of the 10th ACM Conference on Computer and Communications Security*, 272–280. Retrieved from https://sci-hub.do/10.1145/948109.948146

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022

Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in Internet of Things. *Future Generation Computer Systems*, *100*, 144–164. https://doi.org/10.1016/j.future.2019.04.038

Khumoyun, A., Cui, Y., & Hanku, L. (2016). Spark based distributed Deep Learning framework for Big Data applications. *2016 International Conference on Information Science and Communications Technologies, ICISCT 2016*, 1–5. https://doi.org/10.1109/ICISCT.2016.7777390

Kiezun, A., Guo, P. J., Jayaraman, K., & Ernst, M. D. (2009). Automatic creation of SQL injection and cross-site scripting attacks. *Proceedings - International Conference on Software Engineering*, 199–209. https://doi.org/10.1109/ICSE.2009.5070521

Kleinman, A. (2017). The most detailed map of the internet was made by breaking the law. Retrieved from https://www.huffpost.com/entry/internet-map_n_2926934

Komalasari, R. (2020). Manfaat Teknologi Informasi Dan Komunikasi Di Masa Pandemi Covid 19. *Tematik*, *7*(1), 38–50. https://doi.org/10.38204/tematik.v7i1.369

Kozik, R. (2018). Distributing extreme learning machines with Apache Spark for

NetFlow-based malware activity detection. *Pattern Recognition Letters*, *101*, 14–20. https://doi.org/10.1016/j.patrec.2017.11.004

Liou, C. Y., Huang, J. C., & Yang, W. C. (2008). Modeling word perception using the Elman network. *Neurocomputing*, *71*(16–18), 3150–3157. https://doi.org/10.1016/j.neucom.2008.04.030

Lippmann, R. P., Fried, D. J., Graf, I., Haines, J. W., Kendall, K. R., McClung, D., … Zissman, M. A. (2000). Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation. *Proceedings - DARPA Information Survivability Conference and Exposition, DISCEX 2000*, *2*, 12–26. https://doi.org/10.1109/DISCEX.2000.821506

Liu, J., Xiao, Y., & Chen, C. L. P. (2012). Authentication and access control in the Internet of things. *Proceedings - 32nd IEEE International Conference on Distributed Computing Systems Workshops, ICDCSW 2012*, 588–592. https://doi.org/10.1109/ICDCSW.2012.23

Marir, N. (2018). Distributed Abnormal Behavior Detection Approach Based on Deep Belief Network and Ensemble SVM using Spark. *IEEE Access*, 59657–59671.

Marjani, M. (2017). Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges. *IEEE Access*, 5247–5261.

Mavridis, I., & Karatza, H. (2017). Performance evaluation of cloud-based log file analysis with Apache Hadoop and Apache Spark. *Journal of Systems and Software*, *125*, 133–151. https://doi.org/10.1016/j.jss.2016.11.037

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-BaIoT-Network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, *17*(3), 12–22. https://doi.org/10.1109/MPRV.2018.03367731

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. *Journal of Network and Computer Applications*, *36*(1), 42–57. https://doi.org/10.1016/j.jnca.2012.05.003

Mohammadi, M. (2018). Deep Learning for IoT Big Data and Streaming Analytics: A Survey. *IEEE Communications Surveys & Tutorials*, *20*(4), 2923–2960.

Moustafa, N., Slay, J., & Technology, I. (2015). Unsw-nb15: a comprehensive data set for network intrusion detection systems [157] N. Moustafa, J. Slay, Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). *Proceeding Military Communications and Information Systems Conference (MilCIS)*, 1–6. https://doi.org/10.1109/MilCIS.2015.7348942

Munawar, Zen and Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *J-SIKA| Jurnal Sistem Informasi Karya Anak Bangsa*, *02*(01), 14–20.

Mylavarapu, G. (2015). Real-time Hybrid Intrusion Detection System using Apache Storm. *High Performance Computing and Communications IEEE 7th Int. Symp. Cyberspace Safety and Security Conf. Embedded Software and Systems*, 1436–1441. https://doi.org/10.1109/HPCC-CSS-ICESS.2015.241

Nobakht, M., Sivaraman, V., & Boreli, R. (2016). A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow. *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, 147–156. https://doi.org/10.1109/ARES.2016.64

Radoglou Grammatikis, P. I., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things*, *5*, 41–70. https://doi.org/10.1016/j.iot.2018.11.003

Rav, D., Wong, C., Lo, B., & Yang, G. (2017). Deep Learning Approach to on-Node SensorData Analytics for Mobile or Wearable Devices. *IEEE Journal of Biomedical and Health Informatics*, *12*(1), 106–137. https://doi.org/10.1109/JBHI.2016.2633287

Roopak, M., Yun Tian, G., & Chambers, J. (2019). Deep learning models for cyber security in IoT networks. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*, 452–457. https://doi.org/10.1109/CCWC.2019.8666588

Saxe, J. (2015). Deep Neural Network Based Malware Detection using Two Dimensional Binary Program Features. *2015 10th International Conference on Malicious and Unwanted Software (MALWARE)*, 11–20. Retrieved from https://dl.acm.org/doi/10.1109/MALWARE.2015.7413680

Schiffer, A. (2017). How a fish tank helped hack a casino. Retrieved November 2, 2020, from https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

Smith, D. F., Wiliem, A., & Lovell, B. C. (2015). Face recognition on consumer devices: Reflections on replay attacks. *IEEE Transactions on Information Forensics and Security*, *10*(4), 736–745. https://doi.org/10.1109/TIFS.2015.2398819

Sood, A. K. (2013). Crimeware-as-a-service—a Survey of Commoditized Crimeware in The Underground Market. *International Journal of Critical Infrastructure Protection*, *6*(1), 28–38. https://doi.org/10.1016/j.ijcip.2013.01.002

Stolfo, S. J., Fan, W., Lee, W., Prodromidis, A., & Chan, P. K. (2000). Cost-based modeling for fraud and intrusion detection: Results from the JAM project. *Proceedings - DARPA Information Survivability Conference and Exposition, DISCEX 2000*, *2*, 130–144. https://doi.org/10.1109/DISCEX.2000.821515

Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M. (2016). Deep learning approach for Network Intrusion Detection in Software Defined Networking. *Proceedings - 2016 International Conference on Wireless Networks and Mobile Communications, WINCOM 2016: Green Communications and Networking*, 258–263. https://doi.org/10.1109/WINCOM.2016.7777224

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A Detailed Analysis of the KDD CUP 99 Data Set. *Proc. IEEE Symp. Computational Intelligence for Security and Defense Applications*, (Cisda), 1–6. Retrieved from https://sci-hub.do/10.1109/CISDA.2009.5356528

Thilina, A. (2016). Intruder Detection using Deep Learning and Association Rule Mining. *2016 IEEE International Conference on Computer and Information Technology (CIT)*, 615–620.

Trifa, Z., & Khemakhem, M. (2014). Sybil nodes as a mitigation strategy against sybil attack. *Procedia Computer Science*, *32*, 1135–1140. https://doi.org/10.1016/j.procs.2014.05.544

Vavilapalli, V., Murthy, A., … C. D.-P. of the 4th, & 2013, U. (2013). Apache hadoop yarn: Yet another resource negotiator Big Data Resources Scheduling. *The 4th Annual Symposium on Cloud Computing*, 1–16. Retrieved from https://dl.acm.org/citation.cfm?id=2523633

Veen, J. S. van der. (2015). Dynamically Scaling Apache Storm for The Analysis of Streaming Data. *2015 IEEE First International Conference on Big Data Computing Service and Applications*, 154–161. IEEE.

Vimalkumar, K., & Radhika, N. (2017). A big data framework for intrusion detection in smart grids using apache spark. *2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017, 2017-Janua*, 198–204. https://doi.org/10.1109/ICACCI.2017.8125840

Vinayakumar, R. (2019). Deep Learning approach for Intelligent Intrusion Detection System. *IEEE Access*, 41525–41550.

Wang, W. (2017). Hast-ids: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. *IEEE Access*, 1792–1806. https://doi.org/10.1109/ACCESS.2017.2780250

Zaharia, M. (2016). Apache spark: a unified engine for big data processing. *Communications of the ACM*, *59*(ACM), 56–65.