# ANALISIS DAMPAK REVOLUSI INDUSTRI 4.0 TERHADAP KEAMANAN DATA DIGITAL

**Roy Rinaldi[1], Iwan Krisnadi[2]**
[(1)(2)]Program Studi Magister Teknik Elektro, Fakultas Teknik, Universitas Mercubuana
Universitas Mercubuana, Menteng, Jakarta, Indonesia
55419110010@student.mercubuana.ac.id

**Abstrak**
Lahirnya istilah industry 4.0 memasuki babak baru dalam ekosistem bisnis, pemanfaatan teknologi digital *seperti Big Data, Autonomous Robots, Cybersecurity, Cloud, dan Augmented Reality.* Menjadikan pabrik – pabrik berevolusi menjadi smart factory, adanya hal tersebut tentu mampu mendongkrak jumlah produksi serta menimbulkan kedinamisan bisnis. Tak hanya itu saja mau tidak mau pelaku industry tentunya harus menyiapkan strategi untuk menghadapi revolusi industry agar menjaga keberlangsungan bisnis salah satunya yaitu meningkatkan kualitas sumber daya manusia. Dengan gencarnya perubahan lini kehidupan menjadi serba digital, bukan tidak mungkin robot akan menggantikan pekerjaan manusia. Akan tetapi dominasi robot tidak akan terjadi di semua sektor. Oleh karena itu perusahaan perlu mempersiapkan sumber daya manusia yang andal agar tetap mencapai kesuksesan. Industri 4.0 memiliki potensi ancaman baru dari segi keamanan data antara lain targeted attack, penyebaran ransomware, serta insider oleh karena itu baik pelaku bisnis maupun individu harus memiliki kesadaran untuk menjaga kerahasiaan data. Pentingnya peran pemerintah untuk menjamin keberlangsungan industry 4.0 sangat diperlukan. Sebagai contoh pemerintah harus menyediakan regulasi untuk perlindungan data pribadi. Dengan memiliki regulasi tersebut tentunya dapat menekan kebocoran data serta mendukung ekosistem industry 4.0 yang begerak secara dinamis.
Kata Kunci : Industri 4.0, Keamanan Data, Teknologi Informasi, Regulasi, Smart Factory.



## 1. Pendahuluan

### 1.1 Latar Belakang

Dunia industri terus berkembang dari masa ke masa, mulai dari industri 1.0 dimana dimulainya penggunaan mesin uap dalam proses produksi barang. Kemudian pada awal abad ke 20 proses produksi barang meningkat dari penggunaan mesin uap ke tenaga listrik, pada abad ini mulai menggunakan mesin produksi dan sudah mulai perlahan - lahan menggantikan peran manusia, masa tersebut dikenal dengan industri 2.0. Pada akhir abad 20 ditandai dengan kemunculan internet dan teknologi digital, lahirlah industri 3.0 atau dikenal sebagai revolusi digital. Perkembangan teknologi pada industri 3.0 memicu arus pertukaran data yang begitu masif dan penggunaan internet yang makin berkembang. Pada akhrinya tepatnya pada abad 21 lahirlah industri 4.0. Revolusi industri 4.0 merupakan kolaborasi antara teknologi cyber dengan teknologi automation, konsepnya adalah penerapannya berpusat pada otomatiasi yang dilakukan oleh teknologi tanpa memerlukan tenaga kerja manusia dalam proses pengaplikasiannya. Pada era ini ukuran perusahaan tidak menjadi jaminan namun kelincahan perusahaan menjadi kunci keberhasilan meraih kemenangan dengan cepat, contohnya adalah banyak startup berdiri dengan tidak nyaris tidak memiliki aset fisik namun nyatanya bisnisnya hanya mengandalkan teknologi.

Terlepas dari peran teknologi dalam bidang industri, manfaat dengan adanya revolusi industri 4.0 pertukaran informasi dapat dengan mudah dilakukan kapan saja serta dimana saja tanpa batasan waktu hanya dengan jaringan internet. Pemanfaatan IoT, Big Data, serta cloud computing menjadi tanda bahwa sebuah perusahaan bertransformasi ke dunia digital. Revolusi Industri 4.0 dan peningkatan konektivitas antara bisnis dan kehidupan kita sehari-hari kini tengah mendorong transformasi bisnis dan memajukan kehidupan para karyawan dan pelanggan di seluruh dunia. Akan tetapi, ada sisi buruk dari peningkatan mobilitas dan keterhubungan dalam bentuk risiko keamanan yang berkembang secara eksponensial seiring lebih banyak data dan operasi bisnis yang berpindah ke cloud.

### 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan penelitian akan fokus pada,

1. Bagaimana strategi perusahaan di era industri 4.0 dalam mengamankan data ?
2. Bagaimana respon pemerintah dalam industry 4.0 ?

### 1.3 Tujuan dan Manfaat Penelitian

Tujuan dari penelitian ini adalah mengetahui bagaimana industri 4.0 mempengaruhi bisnis pada perusahaan serta apa ancaman yang terjadi pada revolusi industri 4.0.

Manfaat dari penelitian ini adalah dapat memberikan kontribusi ilmiah sebagai rujukan literatur serta memberikan rekomendasi kepada perusahaan tentang tata cara melindungi data ditengah arus informasi yang begitu massif.

## 2. Studi Literatur

Penelitian yang dilakukan oleh perusahaan security McAfee mengatakan bahwa Kejahatan siber terjadi tanpa henti, jumlahnya tidak pernah berkurang dan terjadi begitu masif setiap saat di berbagai belahan dunia. Pelaku kejahatan internet memanfaatkan celah untuk mengeksploitasi sebuah sistem dan meminta sejumlah bayaran atas ulahnya. Mereka bergerak sangat cepat, mengadopsi teknologi cloud serta enkripsi yang sulit untuk diketahui jejaknya. Kejahatan siber semakin berkembang dengan kurangnya security awareness perusahaan terhadap revolusi industri menjadikan perusahaan tersebut menjadi sasaran yang mudah sekali dimonetasi. Bank menjadi target favorit para penjahat dunia maya hal ini telah terjadi lebih dari satu dekade. Kejahatan cyber dapat mengakibatkan kebocoran data nasabah serta uang yang besar. Hal tersebut tentunya menjadi ancaman serius oleh bank serta nasabah yang menyimpan uang. [1].

Selain itu, ThreatMetrix Q2 Cybercrime Report mengungkapkan bahwa wilayah Asia Pasifik dari tahun ke tahun telah mengalami peningkatan sebanyak 45 persen dalam kejahatan siber dan region ini mengalami serangan spoofing tertinggi di dunia terhadap perangkat dan identitas. Dan kabar buruknya lagi Kejahatan siber meningkat 44% pada akhir 2018 [2].

Ketika teknologi di seluruh dunia menjadi lebih sinkron dan dapat dioperasikan, big data akan menjadi inti yang menghubungkan segala sesuatunya. Dengan kemampuan untuk mengumpulkan data internasional dalam volume besar secara efisien, kamu bisa lebih memahami dan mengelola berbagai fenomena. Memanfaatkan revolusi industri 4.0 yang ditandai dengan perkembangan pesat teknologi internet. Big data nantinya akan menyediakan data yang dibutuhkan di dalam revolusi Industri 4.0. Big data untuk memenangi persaingan di berbagai bidang di era revolusi Industri 4.0 ini. Teknologi robot, artificial intelligence, internet of things, hingga big data bisa menggantikan sebagian kebutuhan tenaga manusia. Era internet sering disebut juga era Big Data, Internet of Thing, Disrupsi, Revolusi Industri 4.0. oleh sebab itu jelaslah bahwa big data menjawab tantangan revolusi industri 4.0 [3].

Kemajuan Teknologi Informasi di satu sisi sangat berperan dalam meningkatkan kecepatan dan efisiensi layanan berbagai critical infrstructure tersebut. Namun, di sisi yang lain juga memberikan resiko penyalahgunaan keknologi informasi dan komunikasi dalam bentuk cyber threat tersebut untuk hal-hal yang merusak atau membahayakan, keamanan siber atau cyber security perlu menjadi perhatian penting khususnya dalam menghadapi era revolusi industri 4.0. Secara global dinamika dalam ancaman transaksi data di internet semakin banyak terjadi, ditambah lagi dengan ancaman penyebaran Hoax dan pencurian data pribadi.

Industri 4.0 mencakup tiga tahapan penting antara lain adalah mendapatkan rekaman digital, kemudian memanfaatkan sensor yang melekat pada aset industri dan mengumpulkan data dengan meniru kebiasaan manusia teknologi ini dikenal sebagai sensor fusion. Di era industry 4.0, organisasi atau perusahaan sangat terhubung dengan internet. Hal tersebut tentu saja menguntungkan bagi penjahat cyber yang menemukan banyak titik masuk yang lebih mudah dan tidak aman ke dalam jaringan dan perangkat. Botnet adalah salah satu senjata yang dapat digunakan untuk melakukan serangan DDoS dan crypto-jacking. Serangan publik terhadap critical infrastruture dan sektor industri menjadi semakin sering dan cangguh. Ukraina menjadi salah satu target yang menghadapi banyak serangan pada jaringan mereka, serta memaksa pemadaman listrik di beberapa negara AS [4].

Saat ini, seiring dengan perkembangan teknologi yang semakin canggih membawa dunia memasuki era revolusi 4.0. Big Data, sebagai salah satu komponen penting dalam indutri 4.0, dimanfaatkan oleh sebagian besar perusahaan untuk menganalisis data sehingga mendapatkan gambaran yang jelas mengenai tingkah laku konsumen. Hal ini tentunya dapat membantu perusahaan dalam mengomunikasikan produk atau jasa perusahaannya secara lebih efektif dan tepat sasaran. Namun sayangnya, seringkali data dalam jumlah besar ini disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Tujuan dari artikel konseptual ini adalah untuk memberikan diskusi yang komprehensif tentang ancaman privasi yang muncul dalam Big Data dengan terlebih dahulu melihat keterkaitan antara Internet of Things dengan Big Data. Internet of Things menciptakan volume data yang besar yang kemudian membentuk Big Data. Meskipun teknologi Big Data sangat berguna dalam mempermudah kehidupan, namun disisi lain teknologi ini juga mengancam privasi pengguna dan sulit untuk dijamin keamanannya ketika berhadapan dengan Big Data [5].

Menurut Vitor Jesus dan Mark Josephs, ada empat kunci bahwa industri 4.0 berjalan, tidak lain yaitu cyber-physical system (CPS), Cloud-Assisted Manufacturing, Mobile Technologies dan Augmented Reality serta Big Data, kemudian Artificial Intelligence dan Analytic. Kemudian tantangan dari adanya industri 4.0 sendiri adalah kompleksitas sistem-sistem yang melibatkan beberapa visi teknis dan bisnis yang berbeda membuat transisi ke industri 4.0 belum matang. Oleh karena itu diperlukan kerangka kerja yang mampu mengintegrasikan banyak domain yang terdiri dari paradigma industri baru menuju industri 4.0 [6].

Pada penelitian yang dilakukan oleh Beyzanur Cayir Ervural dan Bilal Ervural berpendapat bahwa transformasi digital yang begitu cepat menyebabkan munculnya industri 4.0 yang erat kaitanya dengan volume data yang begitu besar, pengembangan sistem interaktif manusia dengan mesin dan meningkatkan komunikasi antar lingkungan digital dalam konteks IoT. Dengan industri 4.0 kombinasi antara teknologi informasi dan operasional teknologi telah membawa

tantangan baru. Cyber Security adalah masalah utama bagi pemerintahan di seluruh dunia dan telah mengupayakan untuk melindungi dari berbagai ancaman cyber. Pada tahun 2020 diperkirakan lebih dari 50 juta perangkat IoT telah sadar dengan betapa pentingnya masalah cyber security [7].

## 3. Metodologi Penelitian

Penelitian ini bersifat deskriptif kualitatif, dimana melakukan studi literatur untuk mendapatkan informasi sesuai dengan topic pembahasan serta melakukan review pada vendor security dalam dukungannya pada industry 4.0. Tahapan yang dilakukan dalam penelitian ini adalah sebagai berikut :

1. Mengidentifikasi masalah serta merumuskan masalah.
2. Melakukan studi literatur terkait cyber security pada industry 4.0
3. Melakukan analisa data terkait studi literature yang telah didapat
4. Menarik Kesimpulan

## 4. Hasil dan Pembahasan

Industri 4.0 adalah istilah yang digunakan untuk menggambarkan masa depan produksi industri berdasarkan pemanfaatkan "Internet of Things" atau dikenal dengan IoT. Karakteristiknya meliputi tingkat kemandirian sebuah produksi yang tinggi dan kemampuan secara bersamaan memperhitungkan produksi yang dinamis dan didukung dengan analisa yang akurat. Pabrik berubah menjadi pabrik pintar dan proses yang berlangsung dikendalikan dan dikoordinasikan secara realtime, melintasi batasan yang tidak dapat dilakukan dengan manusia dalam proses produksi. Manufacturing Automation memungkinkan perusahaan di banyak industri menghasilkan produk dengan jumlah besar, namun juga dengan biaya yang rendah untuk memenuhi kebutuhan pelanggan.

Kemudahan akses pada era sekarang, mengakibatkan perusahaan dapat bereaksi secara fleksibel terhadap perkembangan pasar serta perubahan cepat dalam persyaratan produk atau fluktuasi suatu harga komoditas. Tingkat kemampuan adaptasi yang tinggi ini disertai dengan peningkatan kemampuan kapasitas produksi membuat pengelolaan sumberdaya menjadi fleksibel dan berfungsi meniungkatkan efisiensi operasi secara keseluruhan. Perhitungan yang lebih akurat serta analisa yang matang membutuhkan sedikit sumber daya dan memangkas biaya produksi dalam penggunaan human resource.

### 4.1 Strategi Perusahaan Dalam Menghadapi Revolusi Industri

Revolusi industri pertama kali diperkenalkan oleh Prof. Klaus Schwab, Founder and Executive Chairman of the World Economic Forum, di dalam bukunya. Buku tersebut menjelaskan bahwa era revolusi industri 4.0 akan mengubah hampir sebagian besar hidup manusia. Revolusi ini melahirkan super komputer, kendaraan tanpa pengemudi, robot pintar, perkembangan neurotechnology dan dunia digital yang serba otomatis lainnya. Kini realitas di dunia dapat terkoneksi dengan dunia virtual melalui bantuan internet. Ini yang menyebabkan terjadinya berbagai perubahan dalam kehidupan manusia, terutama di dunia bisnis. Kemajuan teknologi yang ada di dalamnya membuat wajah industri dunia berubah secara drastis [8].

Bagi berbagai perusahaan, era revolusi industri 4.0 merupakan fenomena yang mutlak dan tidak bisa dihindari. Perusahaan harus mempunyai strategi yang mampu melakukan transformasi dan inovasi untuk menghadapinya. Ini agar perusahaan dan bisnis yang telah dibangun tidak tergilas oleh zaman dan terhambat perkembangannya. Perusahaan harus sudah memiliki sebuah peta perjalanan yang terintegrasi sehingga arah pengembangan bisnis terlihat dengan jelas. Saat ini pemerintah Indonesia pun telah memunculkan strategi yang membuka jalan menuju Indonesia 4.0. Jika dikaitkan dengan perusahaan, peta strategi yang dikeluarkan ini digadang-gadang sebagai solusi untuk mempercepat pengembangan industri nasional di era digital ini. Berdasarkan peta yang dikeluarkan oleh pemerintah, berikut strategi yang bisa dilakukan perusahaan di era revolusi industri 4.0.

#### 4.1.1 Perbaikan Alur Barang dan Material

Ini merupakan upaya yang dicanangkan pemerintah untuk membantu perusahaan di Indonesia. Upaya perbaikan ini bertujuan untuk mengurangi impor bahan baku dan berbagai komponen produksi pada industri. Selain dapat menghemat pembiayaan, pemanfaatan ini juga diharapkan dapat memacu sumber daya alam Indonesia agar bernilai lebih tinggi. Produksi lokal dari sektor hulu dan menengah semakin ditingkatkan, yang dibarengi dengan peningkatan kapasitas dan percepatan adopsi teknologi.

#### 4.1.2 Peningkatan Kualitas Sumber Daya Manusia

Dengan gencarnya perubahan lini kehidupan menjadi serba digital, bukan tidak mungkin robot akan menggantikan pekerjaan manusia. Akan tetapi dominasi robot tidak akan terjadi di semua sektor. Robot masih belum mampu mengambil alih pekerjaan yang berhubungan dengan interaksi manusia dan juga pengetahuan. Oleh karena itu perusahaan perlu mempersiapkan sumber daya manusia yang andal agar tetap mencapai kesuksesan. Karyawan sebaiknya didorong untuk terus belajar dan meningkatkan pengetahuannya mengenai teknologi. Karena tenaga kerja yang mampu mengaplikasikan dan mengontrol teknologi di masa kinilah yang mampu terus bergerak maju. Hal ini pun didukung oleh pemerintah yang berencana merombak kurikulum pendidikan di Indonesia. Nantinya pendidikan Indonesia lebih menekankan pada Science, Technology, Engineering,

the Arts, dan Mathematics (STEAM), serta meningkatkan kualitas sekolah kejuruan.

#### 4.1.3 Penggunaan Teknologi Digital

Seperti yang diharapkan pemerintah, perusahaan mampu menggunakan teknologi digital seperti Big Data, Autonomous Robots, Cybersecurity, Cloud, dan Augmented Reality. Ini sebagai perwujudan dari tiga solusi pintar dalam menghadapi revolusi industri 4.0, smart foundation, smart process, dan smart connectivity. Perusahaan harus mempunya strategi untuk membangun pondasi IT yang cerdas, membangun proses IT yang cerdas dan membangun sistem konektivitas IT yang cerdas. Jika keseluruhan ini berhasil dilakukan maka akan sangat membantu untuk meningkatkan efisiensi kerja di dalam perusahaan. Bahkan dengan penerapan teknologi ini perusahaan pun akan mampu menghemat biaya sekitar 12-15%..

#### 4.1.4 Harmonisasi Aturan & Kebijakan

Dalam sebuah perusahaan ada banyak proses yang dilalui untuk akhirnya menghasilkan sebuah produk. Dan dalam setiap proses ini ada aturan dan kebijakannya sendiri. Baik yang ditujukan untuk barang dan jasa yang di produksi tersebut, karyawan, manajemen maupun pemangku jabatan. Diperlukan harmonisasi dalam pembuatan dan pengaplikasian aturan dan kebijakan tersebut agar tidak menjadi bumerang bagi perusahaan sendiri. Apalagi pada era revolusi industri dimana berbagai alur dalam perusahaan juga ikut berubah. Aturan dan kebijakan dalam suplai bahan baku, perlindungan karyawan, pembagian kerja, persaingan bisnis, dan masih banyak lagi harus dibuat dengan jelas agar tidak merugikan salah satu pihak. Selain di dalam perusahaan, pemerintah pun ikut membantu dengan melakukan harmonisasi aturan dan kebijakan untuk mendukung daya saing industri dan memastikan koordinasi yang baik dengan pembuat kebijakan.

#### 4.1.5 Menarik Minat Investor Asing

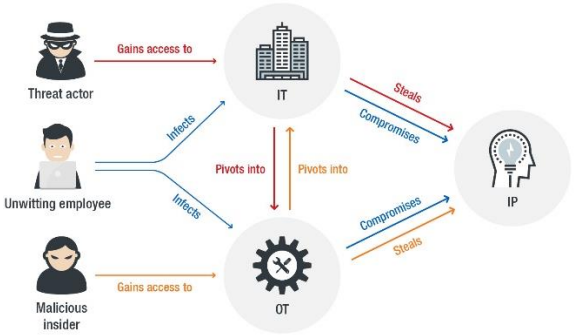
Sebuah bisnis memerlukan investor sebagai penunjang pengembangan perusahaan. Layaknya bisnis yang masih baru, perusahaan yang sedang memasuki era industri 4.0 juga membutuhkan investor untuk membantu. Tidak hanya dari segi materil, investor ini juga dapat dimanfaatkan untuk transfer teknologi. Khususnya investor asing yang sebagian besar telah menjalani perubahan revolusi jauh sebelum perusahaan lokal mengenalnya. Kehadiran investor asing ini sangat membantu negara berkembang seperti Indonesia yang masih lebih sedikit penerapan teknologinya. Untuk mening-katkan investasi, pemerintah Indonesia pun akan secara aktif melibatkan perusahaan manufaktur global. Pemerintah nantinya memilih 100 perusahaan manufaktur teratas dunia sebagai kandidat utama dan menawarkan insentif menarik. Jalan lain yang ditempuh adalah berdialog dengan pemerintah asing untuk kolaborasi tingkat nasional. Upaya ini diharapkan berpengaruh terhadap proses transformasi kegiatan ekonomi industri di Indonesia.

#### 4.1.6 Perluas Jaringan Bisnis

Upaya perluasan jaringan bisnis dapat dilakukan dengan berbagai cara. Tidak hanya membidik investor tetapi juga konsumen. Perluas jaringan perusahaan di kalangan konsumen dengan menyediakan produk yang berkualitas serta layanan yang memuaskan. Dengan kepuasan yang diperoleh, bukan tidak mungkin konsumen itu sendiri yang menjadi pembuka jalan perusahaan Anda dikenal oleh banyak pihak. Dibantu juga dengan melakukan promosi dan mendekatkan diri pada konsumen yang menjadi solusi paling ampuh untuk mempertahankan konsumen. Karena jika konsumen telah percaya pada perusahaan Anda, perubahan pola maupun metode konsumsi sebagai akibat revolusi industri pun tidak akan berpengaruh terlalu banyak kepada mereka.

### 4.2 *Cyber* Security *Industry 4.0*

Dalam revolusi industri keempat, sistem cyber-physical (CPSs) menggabungkan komponen fisik dan jaringan digital untuk mengubah cara perusahaan manufaktur melakukan otomatisasi proses dan berbagi informasi. Didoring oleh Industi Internet of Thinks, Machine Learning, serta Big Data, industri 4.0 mendorong peningkatan yang signifikan terhadap pertukaran data dan kontrol industri dalam manufaktur, seperti munculnya pabrik pintar. Saat ini Information Technology (IT), Operational Technology (OT), dan Intellectual Property (IP) sedang terintegrasi. Dengan munculnya tren tersebut lahir serangkaian masalah keamanan yang dapat mengancam keberlangsungan industri 4.0 [9].




Gambar 1. Mekanisme Industri Manufaktur 4.0

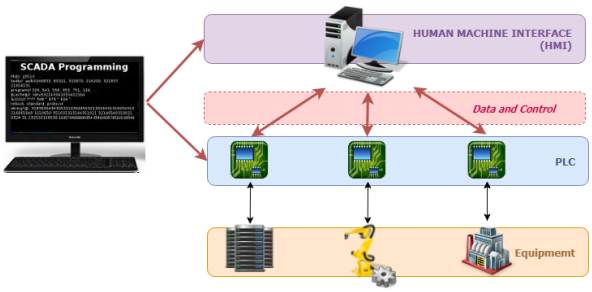
Dengan Mengadopsi industri 4.0, industri manufaktur dapat dianggap sebagai target yang menarik bagi penyerang. Konvergensi dapat dilihat oleh penyerang sebagai kesempatan bergerak secara masif melintasi jaringan manufaktur, kemudian melakukan bypass sistem IT dan OT untuk menginfeksi user. Penyerang dapat mengambil keuntungan dengan menanam malware pada sistem manufaktur sehingga yang terparah dapat melakukan sabotase terhadap produksi.

### 4.3 Potensi Ancaman Cyber

#### 4.3.1 Targeted Attack

Bukan rahasia lagi, manufaktur adalah industri yang menjadi tujuan targeted atttack dalam serangan siber. Menurut studi Enterprise Enviromental Factor (EEF), 48 persen produsen di beberapa titik telah mengalami insiden keamanan, dan setengah dari organisasi tersebut menderita kerugian finansial atau gangguan terhadap bisnis mereka. Menurut survei, industri manufaktur adalah yang paling ditargetkan untuk serangan siber, tepat berada di belakang sektor publik dan bisnis keuangan. Industrial Control System (ICS) atau Supervisory Control And Data Acquisition (SCADA) adalah perangkat lunak yang paling sering digunakan dalam industri manufaktur, infrastruktur dan berbagai bidang lain, merupakan titik terlemah dalam sistem keamanan perusahaan. Contoh kasusnya adalah serangan malware BlackEnergy (2015) dan Industroyer (2016) yang memadamkan listrik di Ukraina atau serangan Stuxnet di Iran [10].

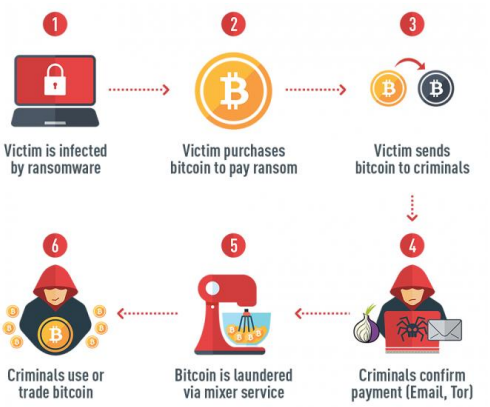
Kasus terbaru adalah GreyEnergy (2018), yang dirancang untuk sasaran lebih luas. Perlu dicatat bahwa ICS/SCADA digunakan bukan hanya di manufaktur, tetapi juga pada pembangkit listrik, perusahaan transmisi, pengolahan minyak dan gas, pabrik-pabrik, bandara sampai layanan pengiriman [11].




Gambar 2. SCADA Illustration System

#### 4.3.2 Ransomware

Menurut laporan Verizon 2018, 56 persen insiden malware melibatkan ransomware sehingga menjadikannya sebagai bentuk malware yang paling umum. Dalam praktiknya, ransomware oleh pengembangnya dikolaborasikan dengan botnet, bahkan CryptoJacking untuk mendapatkan keuntungan ganda. Menghadapi ransomware memang bukan perkara mudah, sehingga bagi sebuah perusahaan memiliki alat proteksi dari ransomware bukan suatu hal yang bisa ditawar karena ransowmare tidak pernah pilih-pilih ketika menyerang korbannya.




Gambar 3. Alur Pembayaran Ransomware

Apabila korban terkena ransomware maka korban harus dipaksa membayar dengan cryptocurency seperti bitcoin maupun yang lain. Dengan demikian korban akan kesulitan melacak penyerang dikarenakan pembayaran tersebut menggunakan rekening sementara untuk setiap transaksinya.

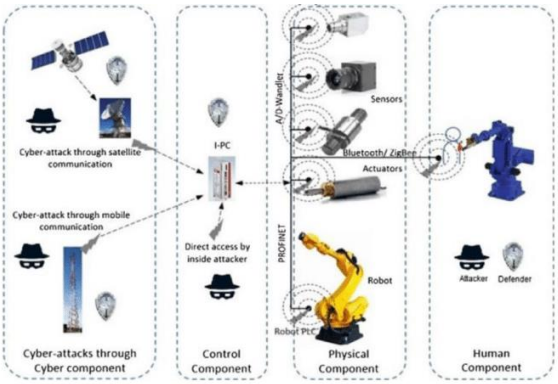
#### 4.3.3 Insider

Menurut salah satu perusahaan antivirus, ada kesenjangan antara pengetahuan karyawan dan perkembangan keamanan siber. Akar masalah dari kerentanan, 52 persen di antaranya dinilai berasal dari kesalahan karyawan yang dilakukan secara tidak sengaja, seperti salah copy file, salah kirim file, meninggalkan komputer dalam keadaan terbuka saat tidak dipakai, dan lain-lain. Ponemon Institute dalam studinya mengatakan, satu dari empat kebocoran data disebabkan oleh orang dalam yang dilakukan sengaja dengan motivasi finansial, spionase dan persaingan bisnis. Untuk menghadapi tantangan keamanan di Industri 4.0, pelaku bisnis diimbau untuk menggunakan solusi keamanan seperti menggunakan antivirus yang premium agar dapat melindungi data secara optimal.

### 4.4 Skenario Serangan Pada Industri 4.0

#### 4.4.1 Skenario Pertama

Penyerang menginstall malicious program kemudian memblokir semua operasi produksi dan logistik . Data produksi dan aplikasi dimanipulasi sehingga dapat menggagalkan proses produksi. Skenario terburuk adalah mesin produksi dapat menyebabkan kerusakan fisik di areanya.




Gambar 4. Manufacture Industry Attack

### 4.4.2 Skenario Kedua

Perintah untuk robot industri dikirim melalui embeded system yang biasanya terhubung ke controller. Saat controller terhubung dengan jaringan, maka penyerang dapat membaca data aplikasi serta sistem. Kemudian menginstal paket yang dirancang untuk mensabotaso jalur produksi atau sistem terkait dan bahkan melumpuhkan seluruh Infrastruktur IT Perusahaan

### 4.4.3 Skenario Ketiga

Sosial Engineering yaitu penyerang mengeksploitasi karakteristik manusia seperti pura - pura meminta bantuan, memanfaatkan kepercayaan serta membuat karyawan tersebut tertarik pada suatu hal dan penyerang dapat mudah mendapatkan sesuatu seperti password login atau informasi rahasia yang dapat digunakan untuk mendapatkan akses ke data pribadi karyawan dan masuk ke sistem utama melalui komputer karyawan. Dengan melakukan social engineering penyerang tidak perlu menghabiskan waktu untuk mencari celah keamanan yang ada pada sebuah sistem.


Gambar 5. Social Engineering Flow

Untuk melindungi data baik perusahaan maupun pribadi, diperlukan kesadaran setiap individu dalam menggunakan internet. Melindungi akun pribadi seperti alamat email maupun akun di marketplace menggunakan autentikasi 2 langkah. Dimana saat password sebuah akun dicuri oleh orang. Maka kita dapat melakukan recovery apabila akun tersebut diaktifkan autentikasi 2 langkah. Kemudian disarankan untuk mencadangkan data penting pada penyimpanan cloud. dengan demikian apabila data kita hilang maka setidaknya ada backup yang dapat digunakan.

### 4.5 Strategi Pemerintah Dalam Menghadapi Industri 4.0

Kehadiran revolusi industri Industri 4.0 sudah tidak dapat di elakkan lagi. Indonesia perlu mempersiapkan langkah strategis agar mampu beradaptasi dengan era industri digital. Indonesia berkomitmen untuk membangun industri manufaktur yang berdaya saing global melalui percepatan implementasi Industri 4.0. Hal ini ditandai dengan peluncuran Making Indonesia 4.0 sebagai sebuah roadmap(peta jalan) dan strategi Indonesia agar dapat memasuki era digital ini. Dengan menerapkan Industri 4.0, Menteri Perindustrian menargetkan, aspirasi besar nasional dapat tercapai. Industri 4.0 melalui konektivitas dan digitalisasinya mampu meningkatkan efisiensi rantai manufaktur dan kualitas produk. Namun di sisi lain digitalisasi industri ini akan berdampak negatif pada penyerapan tenaga kerja dan mengacaukan bisnis konvensional.

Pemerintah harus mengantisipasi dampak negatif dari Industri 4.0. Pada saat pemerintah memutuskan untuk beradaptasi dengan sistem Industri 4.0, maka pemerintah juga harus memikirkan keberlangsungannya. Jangan sampai penerapan sistem industri digital ini hanya menjadi beban karena tidak dapat dimanfaatkan secara optimal. DPR RI perlu mendorong pemerintah untuk mempersiapkan berbagai hal yang berkaitan dengan penerapan Industri 4.0 yang sudah tidak dapat dielakkan lagi. Selain itu DPR RI sebagai lembaga legislasi perlu mempersiapkan payung hukum yang akan mengatur penerapan sistem baru tersebut. hal ini sangat penting untuk mengantisipasi dampak negatif dari revolusi industri ini terhadap industri, ekonomi, pemerintahan, dan politik di Indonesia.

Ada empat langkah strategi yang harus dilakukan pemerintah dalam mengahadapi era revolusi industri 4.0, yaitu:

a. Langkah Pertama, Mendorong angkatan kerja di Indonesia terus belajar dan meningkatkan keterampilannya untuk memahami penggunaan teknologi internet of things atau mengintegrasikan kemampuan internet dengan lini produksi di industri.
b. Langkah kedua, pemanfaatan teknologi digital untuk memacu produktivitas dan daya saing bagi industri kecil dan menengah sehingga mampu menembus pasar ekspor melalui program e-smart.

c. Langkah Ketiga, industri nasional dapat menggunakan teknologi digital seperti Big Data, Autonomous Robots, Cybersecurity, Cloud, dan Augmented Reality. "SistemIndustry 4.0 ini akan memberikan keuntungan bagi industri, misalnya menaikkan efisiensi dan mengurangi biaya sekitar 12-15 persen. sejumlah sektor industri nasional telah memasuki era Industry 4.0, di antaranya industri semen, petrokimia, otomotif, serta makanan dan minuman.
d. Dan langkah keempat, yang diperlukan adalah inovasi teknologi melalui pengembangan startup dengan memfasilitasi tempat inkubasi bisnis. Upaya ini telah dilakukan Kementerian Perindustrian dengan mendorong penciptaan wirausaha berbasis teknologi yang dihasilkan dari beberapa technopark yang dibangun di beberapa wilayah di Indonesia, seperti di Bandung (Bandung Techno Park), Denpasar (TohpaTI Center), Semarang (Incubator Business Center Semarang), Makassar (Makassar Techno Park - Rumah Software Indonesia, dan Batam (Pusat Desain Ponsel).

Hal di atas merupakan Strategi indonesia dalam menghadapi revolusi industri 4.0. Pada saat pemerintah memutuskan untuk beradaptasi dengan sistem Industri 4.0, maka pemerintah juga harus memikirkan keberlangsungannya. Jangan sampai penerapan sistem industri digital ini hanya menjadi beban karena tidak dapat dimanfaatkan secara optimal. Banyak hal yang harus dipersiapkan seperti peran para pengambil keputusan, tata kelola, manajemen risiko implementasi sistem, akses publik pada teknologi, dan faktor keamanan sistem yang diimplementasikan.

Selain itu pemerintah juga harus mempersiapkan sistem pendataan yang berintegritas, menetapkan total harga atau biaya kepemilikan sistem, mempersiapkan payung hukum dan mekanisme perlindungan terhadap data pribadi, menetapkan standar tingkat pelayanan, menyusun peta jalan strategis yang bersifat aplikatif dan antisipatif, serta memiliki design thinking untuk menjamin keberlangsungan industri.

## 5. Kesimpulan

Dunia industri terus berkembang dari masa ke masa sesuai dengan perkembangan teknologi. Dimulai dari industri 1.0 dimana pada masa itu mesin uap digunakan dalam produksi barang. Kemudian pada awal abad 20 penggunaan mesin uap mulai ditinggalkan dan beralih ke tenaga listrik. Kemudian pada industri 2.0 peran manusia perlahan - lahan tergantikan oleh mesin produksi. Kemudian pada era industri 3.0 atau dikenal dengan revolusi digital. Perkembangan teknologi pada industri 3.0 memicu arus pertukaran data yang begitu masif. Pada abad 21 lahirnya industri 4.0 mengkolaborasikan antara teknologi cyber dengan dengan teknologi automation.

Revolusi Industri 4.0 menerapkan konsep automatisasi yang dilakukan oleh mesin tanpa memerlukan tenaga manusia dalam pengaplikasiannya. Dimana hal tersebut merupakan hal vital yang dibutuhkan oleh para pelaku industri demi efisiensi waktu, tenaga kerja, dan biaya. Penerapan Revolusi Industri 4.0 di pabrik-pabrik saat ini juga dikenal dengan istilah Smart Factory. Pelaku industri harus menyusun strategi untuk mengikuti arus revolusi industri salah satunya dengan cara penggunaan teknologi digital. Seperti yang diharapkan pemerintah, perusahaan mampu menggunakan teknologi digital seperti Big Data, Autonomous Robots, Cybersecurity, Cloud, dan Augmented Reality. Hal tersebut sebagai solusi cerdas untuk menghadapi revolusi industri 4.0.

Dengan penggunaan teknologi informasi yang bisa dibilang menjadi kebutuhan primer untuk saat ini. Tentunya hal tersebut memiliki ancaman yang tak dapat dihindarkan, keterbukaan informasi yang begitu luas menuntut pelaku industri untuk melindungi data perusahaan maupun data pribadi. Potensi ancaman yang dilahirkan antara lain adalah Targeted Attack, Serangan Ransomware serta Insider. Ketiga hal tersebut harus diwaspadai oleh pelaku industri demi keberlangsungan bisnis. Baik individu maupun perusahaan harus memiliki plan atau mitigasi apabila terjadi ancaman, salah satunya yaitu memiliki cadangan data pada penyimpanan cloud serta para stakeholder harus memiliki kesadaran mengenai keamanan data.

Pentingnya peran pemerintah untuk menjamin keberlangsungan industry 4.0 sangat diperlukan. Sebagai contoh pemerintah harus menyediakan regulasi untuk perlindungan data pribadi. Dengan memiliki regulasi tersebut tentunya dapat menekan kebocoran data dan individu menjadi aman. Bukan hanya dari sisi keamanan data saja yang harus diperhatikan. Pemerintah juga harus mempunyai basis data terpadu yang dapat dimanfaatkan oleh pelaku bisnis agar semuanya dapat saling terintegrasi. Dengan demikian dapat terciptanya ekosistem indsutri yang mampu mendorong percepatan ekonomi.

## Daftar Pustaka

[1] J. Lewis, “Economic Impact of Cybercrime – No Slowing Down,” no. February, pp. 1–28, 2018.

[2] R. Cattanach, “OPINI: Keamanan Siber untuk Revolusi Industri 4.0, Pelajaran Bagi Indonesia,” 2019. [Online]. Available: https://www.liputan6.com/tekno/read/3893138/opini-keamanan-siber-untuk-revolusi-industri-40-pelajaran-bagi-indonesia.

[3] D. Sawitri, “Jurnal ilmiah maksitek issn. 2655-4399,” vol. 4, no. 3, pp. 1–9, 2020.

[4] “Cybersecurity.”

[5] A. E. Syafrina, “ANCAMAN PRIVASI

DALAM BIG DATA Tentu saja tantangan dalam Big Data," pp. 138–149, 2018.

[6] V. Jesus and M. Josephs, "Challenges in Cybersecurity for Industry 4 . 0."

[7] B. C. Ervural and B. Ervural, "Overview of Cyber Security in the Industry 4.0 Era," *Springer Ser. Adv. Manuf.*, no. January, pp. 1–283, 2018.

[8] K. Schwab, "The Fourth Industrial Revolution: what it means and how to respond," *World Econ. Forum*, 2016.

[9] Trend Micro Research, "Security in the Era of Industry 4.0: Dealing With Threats to Smart Manufacturing Environments," 2019. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-in-the-era-of-industry-4-dealing-with-threats-to-smart-manufacturing-environments.

[10] H. Flatt, S. Schriegel, J. Jasperneite, H. Trsek, and H. Adamczyk, "Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements," in *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, 2016.

[11] A. Khalid, P. Kirisci, Z. H. Khan, Z. Ghrairi, K. D. Thoben, and J. Pannek, "Security framework for industrial collaborative robotic cyber-physical systems," *Comput. Ind.*, 2018.