PACE . 2021

DIPLOMASI SIBER DAN TEKNOLOGI MOBILE PADA MULTIDISIPLIN

PENULIS

MUHAMMAD RIDHA ISWARDHANA, S.I.P., M.A.

SUYUD WIDIONO, S.PD., M.KOM.

REVIEWER

DR. SITI MUTIAH SETIAWATI, M.A.

SUHIRMAN, PH.D.

DIPLOMASI SIBER DAN TEKNOLOGI MOBILE PADA MULTIDISIPLIN

Muhammad Ridha Iswardhana, S.I.P., M.A.
Suyud Widiono, S.Pd., M.Kom.

Reviewer:
Dr. Siti Mutiah Setiawati, M.A.
Suhirman, Ph.D.

PACE
Tahun 2021

Sanksi Pelanggaran Pasal 72:
Undang-Undang Nomor 19
Tahun 2002 tentang Hak Cipta

Barangsiapa dengan sengaja dan tanpa hak melakukan perbuatan sebagaimana dimaksud dalam Pasal 2 ayat (1) atau Pasal 49 ayat (1) dan ayat (2) dipidana dengan pidana penjara masing-masing paling singkat 1 (satu) bulan dan/atau denda paling sedikit Rp1.000.000,00 (satu juta rupiah), atau pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Barangsiapa dengan sengaja menyiarkan, memamerkan, mengedarkan, atau menjual kepada umum suatu Ciptaan atau barang hasil pelanggaran Hak Cipta atau Hak terkait sebagaimana dimaksud pada ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).

DIPLOMASI SIBER DAN TEKNOLOGI MOBILE PADA MULTIDISIPLIN

Muhammad Ridha Iswardhana, S.I.P., M.A.
Suyud Widiono, S.Pd., M.Kom.

Reviewer:
Dr. Siti Mutiah Setiawati, M.A.
Suhirman, Ph.D.

PACE
Tahun 2021

Judul:
DIPLOMASI SIBER DAN TEKNOLOGI MOBILE PADA MULTIDISIPLIN

Penulis : Muhammad Ridha Iswardhana, S.I.P., M.A.
Suyud Widiono, S.Pd., M.Kom.

Reviewer : Dr. Siti Mutiah Setiawati, M.A.
Suhirman, Ph.D.

Pertama kali diterbitkan dalam Bahasa Indonesia

oleh
PACE
Partnership for Action on Community Education
Komplek Pondok Pinang Kota
Padang-Sumatera Barat

Cetakan Pertama: Agustus 2021

ISBN: 978-623-97711-0-2

KATA PENGANTAR

Kejahatan siber terus berkembang hingga merusak sistem informasi yang diandalkan untuk transaksi elektronik dengan cara merusak sistemnya dalam bentuk virus, mal ware, craching, dan hacking. Dengan latar belakang kejahatan-kejahatan siber ini pemerintah Indonesia berupaya untuk memberi perlindungan pada pengguna dan mencegah kejahatan terus berkembang. Upaya tersebut melalui Undang Undang ITE (Undang-Undang Informasi dan Transaksi Elektronik) No 11 tahun 2008 yang kemudian diperbaharui dengan UU No 19 tahun 2016. Isi dari Undang Undang ini yang utama berisi tentangan larangan dan sangsi terhadap berbagai kegiatan yang berkaitan dengan pemanfaatan teknologi informasi dan komunikasi. Selamat membaca buku ini, semoga bermanfaat.

Yogyakarta, Juli 2021
Dosen Ilmu Hubungan Internasional
FISIPOL,UGM

Dr. Siti Mutiah Setiawati, M.A.

KATA PENGANTAR

Perkembangan teknologi informasi yang sangat pesat membawa banyak pengaruh positif dan negatif. Pertukaran sebuah informasi yang menjadi lebih mudah dan cepat. Keamanan Informasi bagi pengguna teknologi informasi sangatlah penting. Pembangunan Teknologi Informasi dan Komunikasi dapat mendorong pertumbuhan ekonomi dan secara tidak langsung dapat menciptakan kemandirian dan daya saing bangsa. Oleh karena itu, *Security Information Technology* (IT) harus diperkuat guma menjamin keamanan Informasi. Jangan menyepelekan keamanan informasi. Berbagai teknik/metode untuk meningkatkan keamanan terus dipembangkan oleh para ahli/peneliti.

Peran pemangku kepentingan keamanan siber berpengaruh besar dalam implementasi kebijakan keamanan siber. Pengelola sistem/teknologi memiliki peran strategis dalam menyelenggarakan *IT Security Assesment* di instansinya masing-masing. Melalui *IT Security Assesment,* bisa diketahui risiko keamanan IT yang dapat mengontrol keamanan yang diperlukan bagi organisasi. Dengan adanya buku ini diharapkan para pembaca paham sekali dengan pentingnya keamanan data.

Yogyakarta, 29 Juni 2021
Ketua Lembaga Penelitian & Publikasi UTY

Suhirman, Ph.D

KATA PENGANTAR

Segala Puji dan Syukur kami panjatkan kepada Allah SWT karena atas kemudahan yang diberikanNYAlah buku ini dapat terselesaikan dengan baik.

Buku ini terbagi tersusun dari dua latar belakang keilmuan, yang pertama membahas tentang diplomasi siber dan upaya perlindungan terhadap Ancaman penggunaan teknologi informasi di Indonesia, dan yang kedua membahas tentang teknologi mobile.

Harapannya buku ini dapat menjadi referensi kepada masyarakat luas tentang teknologi yang sedang marak belakangan ini.

Ucapan terimakasih yang sebesa-besarnya tak lupa kami sampaikan kepada para Reviewer dan teman –teman yang telah membantu terpublishnya buku ini.

Yogyakarta, Juli 2021
Tim penulis

DAFTAR ISI

DIPLOMASI SIBER DAN UPAYA PERLINDUNGAN TERHADAP ANCAMAN PENGGUNAAN TEKNOLOGI INFORMASI DI INDONESIA

Muhammad Ridha Iswardhana, S.I.P., M.A.,

Beliau merupakan lulusan Universitas Gadjah Mada pada S1 Departemen Ilmu Hubungan Internasional pada tahun 2015 dan mendapatkan gelar Master of Arts (M.A.) S2 Ilmu Hubungan pada tahun 2017. Sejak tahun 2017 hingga saat ini bergabung menjadi dosen tetap di Prodi Ilmu HI Universitas Teknologi Yogyakarta (UTY). Beliau juga tergabung dalam Asosiasi Ilmu Hubungan Internasional Indonesia (AIHII) dan Emerging Indonesia Project (EIP) serta Alumni INDEF School of Political Economy (ISPE) XXI.

Perkembangan teknologi informasi sudah menjadi hal yang tidak bisa dipisahkan dalam masyarakat Indonesia. Adanya Pandemi *Corona Virus Disease* (COVID-19) turut meningkatkan penggunaan TIK yang diwakili dengan adanya pemanfaatan internet oleh hampir semua orang. Tercatat sebanyak 202 Juta dari 274 Juta populasi di Indonesia telah terhubung dengan internet melalui berbagai sarana (Republika, 2021). Berawal dari gaya hidup yang menjadi sebuah kebiasaan dan berkembang menjadi kebutuhan yang sangat erat dalam kehidupan sehari-hari. Perkembangan *smartphone*, laptop, *tablet*, *smart tv* hingga *smartwatch* membuat masyarakat menjadi lebih ‘melek’ terhadap teknologi informasi. Keberadaan transaksi pembayaran, *marketplace*, dan

berbagai jasa pelayanan secara daring juga mendorong teknologi informasi menjadi sangat luas digunakan.

Berbeda saat akhir dekade 2010-an ketika internet hanya sebatas hiburan dan kebutuhan tambahan, namun saat ini dapat dikatakan sebagai salah satu unsur yang sering dibutuhkan selain sandang, pangan, papan, pendidikan, dan kesehatan. Kemudahan akses, kecepatan pelayanan, dan biaya yang lebih terjangkau menjadi pertimbangan dalam penggunaan internet. Apalagi saat dunia dihadapkan pada fenomena Pandemi COVID-19 yang menyebabkan masyarakat disarankan untuk lebih banyak di rumah menjadi faktor pendorong internet semakin familiar di Indonesia (Kompas.com, 2020). Kebiasaan baru pasca Pandemi COVID-19, utamanya dalam hal *Work From Home* (WFH), *School From Home* (SFH), dan *Virtual Meeting* menyebabkan teknologi informasi telah bergeser menjadi kebutuhan utama. Ketiga kebiasaan baru secara daring tersebut selanjutnya menyebabkan masyarakat menjadi ketagihan terhadap internet.

Lalu, saat ini hampir seluruh lapisan masyarakat telah menjadi pengguna internet, mulai dari anak kecil, remaja, hingga orang tua. Secara sarana, sebanyak 195,3 juta orang atau setara 94,6% internet diakses melalui *smartphone* dengan rata-rata mengakses selama 8 jam 52 menit setiap harinya. Sementara rata-rata kecepatan internet di Indonesia mencapai 23,32 mbps bagi pengguna jaringan fiber optik dan 17,2 mbps untuk jaringan seluler (Kompas, 2021).Terkait profesi, pengguna dunia maya di Indonesia telah menyasar berbagai kalangan, mulai dari pengusaha, mahasiswa, pelajar, pegawai, hingga ibu rumah tangga. Secara jumlah pengguna internet cenderung masih terpusat di Pulau Jawa, lalu diikuti masyarakat di Pulau Sumatra, Sulawesi, Kalimantan, dan pulau-pulau lainnya sebagaimana realitas jumlah penduduk Indonesia. Berbagai kenyataan tersebut dapat dilihat sebagai “dua sisi mata uang”, yakni peluang dan tantangan. Bahwa adanya kemudahan dan efektivitas dalam

berbagai hal juga diikuti oleh adanya ancaman kejahatan dunia maya (Danuri dan Suharwi, 2017).

Ancaman Kejahatan Siber di Indonesia

Berkaca dari realitas sebagai negara dengan latar belakang pengguna internet terbesar keempat di dunia, Indonesia masih menghadapi banyak tantangan yang perlu segera untuk diselesaikan bersama. Jika menilik pada kondisi geografis dan demografi penduduk, maka Indonesia cenderung sangat rawan terhadap ancaman teknologi informasi. Selain itu, banyak dari masyarakat yang 'latah' dalam penggunaan teknologi menyebabkan internet justru bisa menjadi sarana bagi tindakan kejahatan. Adanya fenomena hoaks, ujaran kebencian, terorisme, penipuan daring, dan kejahatan siber menjadi lima ancaman terbesar terhadap pemakaian teknologi informasi (Infokomputer, 2021).

Hoaks menjadi dampak buruk pertama adanya kemudahan penyebaran informasi seiring kemajuan teknologi informasi. Keberadaan berita yang disebarluaskan menggunakan sarana secara daring pada platform internet justru disalahgunakan oleh masyarakat untuk menyebarkan berita bohong. Hoaks dapat dipahami sebagai produk berita bohong dan upaya untuk menipu pembaca agar mempercayai sesuatu hingga dapat membuat opini masyarakat dalam sebuah komunitas tertentu. Penyebaran berita bohong paling banyak terjadi pada media sosial mencapai 92,40% yang menunjukkan bagaimana interaksi komunikasi menjadi rentan untuk digunakan sebagai upaya memecah belah masyarakat. Rendahnya literasi dan kebiasaan masyarakat mempercayai mitos menjadi penyebab utama hoaks banyak terjadi di Indonesia. Apalagi terdapat peristiwa Pemilihan Umum (Pemilu) 2014 dan 2019 menjadikan media sosial dianggap sebagai sumber informasi bagi sebagian masyarakat. Ketika kebiasaan membaca masih rendah sementara harus berhadapan dengan

berkembangnya berita melalui media daring, maka banyak dari warga mudah mengambil kesimpulan tanpa mencoba mencari tahu lebih lanjut terlebih dahulu (Juditha, 2018).

Belum lagi hoaks digunakan sebagai penghasilan ekonomi bagi kelompok tertentu untuk menjelek-jelekkan kalangan atau kelompok tertentu menjadikan hoaks tumbuh subur di negara ini. Akibatnya, terjadi kerusuhan di Wamena, Papua pada 2019 yang diakibatkan oleh adanya isu rasisme yang direspon dengan aksi demonstrasi oleh mahasiswa yang berujung ricuh dan menyebabkan 16 warga setempat meninggal dunia menjadi korban (Jawa Pos, 2019). Meskipun begitu, secara garis besar masyarakat saat ini telah terbagi menjadi dua kelompok, yakni: kelompok yang dianggap mempercayai hoaks sebagai kebenaran dan komunitas yang sudah mendalami apakah hal tersebut merupakan berita bohong semata.

Ujaran kebencian menyusul sebagai ancaman kedua terhadap keberadaan teknologi internet di Indonesia. Ujaran kebencian ini terjadi karena belum disadarinya batasan-batasan dalam penggunaan media sosial dan ketidaktahuan terhadap aturan dalam bermedia sosial (Febriansyah & Purwinatro, 2020). Meskipun sering dianggap serupa dengan hoaks karena banyak disebarluaskan pada media sosial dan berita daring, namun ujaran kebencian memiliki perbedaan mendasar. Ujaran kebencian dapat dipahami sebagai usaha dengan sengaja menyalahgunakan kebebasan ruang publik untuk menyerang dan merusak seseorang, kelompok, lembaga, atau institusi tertentu karena adanya perbedaan tertentu. Ujaran kebencian ini sangat bertentangan dengan budaya santun ketimuran dan Ideologi Pancasila yang dianut masyarakat Indonesia. Upaya penghinaan, pencemaran nama baik, dan memprovokasi masyarakat memiliki makna buruk dan tendensi kebencian merupakan beberapa ciri dari ujaran kebencian (Ningrum dkk, 2018).

Hak untuk kebebasan berekspresi dan keberadaan ruang publik ‘ditunggangi’ oleh kelompok-kelompok tertentu yang memiliki modal ekonomi dan kemampuan menyebarkan informasi yang tidak baik. Sentimen pemikiran, pandangan politik, kepentingan politis, kesenjangan ekonomi, prasangka buruk, rasa benci, dendam, dan polarisasi dalam masyarakat menyebabkan ujaran kebencian sering menyebar luas. Perbedaan latar belakang dan kelompok yang memiliki kepentingan yang berbeda menyebabkan adanya upaya untuk membentuk cara berpikir masyarakat untuk membenci kelompok yang dianggap lawan dengan penggunaan ujaran kebencian. Tidak hanya mengancam bagi demokrasi di Indonesia, namun hal ini juga berakibat buruk terhadap persatuan dan kesatuan masyarakat. Dampaknya, terjadi kerusuhan di Tolikara, Papua akibat penyebaran ujaran kebencian di media sosial pada 2017 (Kusumasari & Arfianto, 2020).

Terorisme dan radikalisme menjadi sisi gelap berikutnya terhadap kemudahan teknologi informasi secara global, utamanya di Indonesia. Keberadaan kedua hal tersebut yang tidak hanya berhasil mengancam kehidupan masyarakat dalam dunia nyata, namun ternyata berimbas pula pada dunia maya. Jika awalnya para teroris berhasil menciptakan kekhawatiran dan rasa takut melalui aksi bom, penyerangan, dan berbagai usaha kekerasan lain. Selanjutnya, media sosial menjadi upaya perjuangan baru yang sedang digunakan untuk menyebarkan paham-paham radikalisme seiring dengan signifikansi pemanfaatan teknologi informasi. Ketika media massa dan media sosial sama-sama menggunakan sarana internet, kelompok teroris tersebut berusaha untuk “membuat panggung” mereka sendiri. Dengan menciptakan pemberitaan sepihak yang menggunakan sisi emosional dan kesamaan latar belakang agama tertentu menjadi usaha publikasi oleh para kelompok pro-kekerasan tersebut. Propaganda menyesatkan tersebut menargetkan para remaja dan generasi

muda yang labil, cenderung kurang mendalami Islam, dan mudah untuk dihasut dengan label agama tertentu (Fahmi, 2018).

Kelompok teroris berusaha untuk memperoleh kepercayaan dan dukungan dari para pembaca secara daring untuk melawan pemberitaan konvensional maupun ideologi yang dianggap bertentangan dengan mereka. Penggunaan situs, penayangan video, unggahan foto, dan fasilitas pesan singkat yang bermuatan kekerasan dan radikalisme menjadi usaha kelompok terorisme untuk menunjukkan eksistensi dan menyebarkan ideologinya (Junaedi, 2010). Pengaruh paling berbahaya atas keberadaan terorisme dalam penggunaan internet dan media sosial adalah sebagai upaya untuk merekrut anggota baru agar dapat melakukan serangan teror berikutnya. Perkembangan *Islamic State of Iraq and Syria* (ISIS) pada 2014 yang kemudian tumbuh menjadi organisasi terorisme besar dapat terjadi akibat penggunaan media Twitter dalam rekrutmen milisi mereka. Dengan memuat ajakan untuk bergabung yang 'dilabeli' atas nama Jihad menggunakan berbagai media sosial berhasil mengajak ribuan anggota setiap tahunnya dari seluruh dunia. Adanya kemudahan internet memungkinkan ISIS untuk mengendalikan propaganda dan rekrutmen para calon anggota tanpa harus bertemu langsung. Serangan Bom Thamrin di Jakarta pada 2016 dan Penyerangan Polrestabes Surabaya tahun 2018 dapat menunjukkan bagaimana bahayanya penyalahgunaan teknologi informasi oleh kelompok terorisme dan radikalisme, bahwa serangan bom terjadi di Indonesia sementara pimpinan kelompok ISIS berada di Suriah dan Irak (Nuruzzaman, 2018).

Penipuan daring kemudian sebagai ancaman penyalahgunaan teknologi informasi dalam hal kegiatan dan transaksi ekonomi. Seiring dengan kemudahan dan efisiensi teknologi informasi mendorong peningkatan kegiatan perekonomian secara digital. Kebutuhan dan pasar yang tidak lagi berbentuk fisik membuat gaya hidup baru dalam bertransaksi secara elektronik. Mulai dari perdagangan barang hingga jasa

semuanya sudah dapat dilakukan secara daring hanya dengan menggunakan jari pada *smartphone*. Berbagai perkembangan tersebut kemudian juga berbanding lurus dengan peningkatan kejahatan penipuan daring. Data menunjukkan apabila 48% konsumen menjadi korban kejahatan penipuan siber, dengan 6% diantaranya telah menjadi korban dan mengalami kehilangan uang. Sementara rata-rata kerugian ditaksir mencapai Rp 3,6 Juta dengan 54% diantaranya berhasil memperoleh uangnya kembali secara utuh.

Dalam modus operandinya, penipuan daring dapat berbentuk beberapa macam, antara lain: Penipuan dengan situs palsu, surel palsu, penggunaan telepon, pengiriman SMS, dan media kartu kredit. Beberapa contoh bentuk penipuan secara siber, diantaranya: mengirimkan pesan apabila memenangkan hadiah, meminta informasi penting seperti sandi rahasia, dan menghubungi untuk mengabarkan apabila ada kerabat yang dirampok, namun semuanya akan berujung pada upaya memperdaya calon korban untuk mengirimkan sejumlah uang dengan berbagai alasan (Samudra, 2019).

Bentuk penipuan lainnya adalah dengan menjual produk dengan harga di bawah harga rata-rata dengan media internet. Tidak jarang banyak korban penipuan yang mudah tergiur akibat tergoda harga yang murah, namun justru memperoleh barang yang tidak sesuai atau bahkan sama sekali tidak mendapatkan produk yang dipesan. Banyak penyebab penipuan secara daring masih sering ditemui pada media internet, misalnya: faktor ekonomi, kurangnya pengalaman, ketidaktahuan akan ancaman penipuan, rendahnya kesadaran terhadap kepatuhan hukum, dan transaksi digital tanpa perlindungan (Sumenge, 2013). Penting bagi masyarakat untuk dapat mengakses edukasi sebelum melakukan transaksi digital agar terhindar dari ancaman penipuan secara siber.

Kejahatan siber yang memiliki banyak sarana. Ancaman kejahatan ini dapat berbentuk serangan virus, *malware*, *cracking*, *hacking*,

dan usaha-usaha lainnya. Sebagai contoh, Indonesia sempat menjadi tujuan paling banyak kedua setelah Tiongkok dalam serangan *malware Ransomware* dan *Wannacry* pada tahun 2018. Bahkan, Indonesia berada di atas Australia, Hongkong, dan Singapura yang mengalami serangan kejahatan siber tersebut (Bisnis.com, 2019). Serangan tersebut paling banyak terjadi ketika masyarakat mengakses situs dan surel yang dengan sengaja berisi kedua virus maupun malware tersebut yang meningkat 4x lipat dibandingkan tahun sebelumnya (Liputan6, 2019). Berbagai ancaman kejahatan siber tersebut bertujuan untuk dapat menyadap transaksi keuangan maupun memperoleh data pribadi. Apabila sebuah perangkat telah terinfeksi virus dan *malware* tersebut, maka dengan mudah pelaku dapat mendapatkan data rahasia secara pribadi yang bisa saja disalahgunakan atau bahkan menjadi korban pemerasan. Tidak jarang kemudian berujung pada penguasaan surel, media sosial, bahkan kartu kredit korban yang berujung pada kejahatan penipuan dan pemerasan.

Ancaman paling besar dari kejahatan siber adalah jika ditujukkan terhadap pejabat publik, petinggi militer, atau pimpinan lembaga negara yang dapat memperoleh data penting dan rahasia negara. Contoh lainnya adalah saat Korea Selatan mengalami serangan yang diduga dilakukan oleh Korea Utara yang berhasil melumpuhkan sebagian sektor perbankan pada tahun 2014 (Suara.com, 2014). Berkaca pada hal tersebut, kejahatan siber sangat berbahaya bagi setiap negara yang berpotensi mengganggu berbagai objek vital seperti sektor keuangan,kelistrikan, navigasi, transportasi, bahkan militer.

Upaya Perlindungan Siber oleh Pemerintah Indonesia

Berkaca pada berbagai ancaman di atas maka dapat dipahami bahwa kehadiran teknologi informasi memberikan perubahan terhadap kehidupan manusia. Apabila sebelumnya setiap orang lebih banyak

berinteraksi dan melakukan banyak kegiatan di dunia nyata, sebaliknya saat ini masing-masing individu telah familiar untuk menggunakan dunia maya guna memenuhi banyak kebutuhan. Kemajuan teknologi mendorong masyarakat untuk dapat mengakses dan menyebarluaskan bermacam informasi secara bebas melalui internet. Internet menjadi ruang baru bagi komunitas untuk saling berbagi data, menyampaikan pendapat, hingga mengikuti gaya hidup yang sedang berkembang. Akan tetapi banyak kemudahan tentunya akan menimbulkan beraneka ancaman, mengingat saat ini keberadaan internet telah mengaburkan terkait batasan dan kejelasan dalam penggunaan internet (Chotimah; Iswardhana; Pratiwi, 2019).

Bahwa kehidupan pada era globalisasi di internet berbeda dengan aktivitas di dunia nyata karena dapat diakses siapa pun, kapan pun, dan dimana pun. Terdapat potensi dan resiko persinggungan antara satu individu terhadap individu lain, baik dalam hal kerjasama ataupun sebaliknya konflik. Perbedaan latar belakang antar pengguna internet juga dapat semakin memperbesar potensi keuntungan maupun resiko kerugian. Keberadaan unsur anonimitas pada dunia maya menjadikan perbedaan mendasar terhadap dunia nyata yang mendorong banyak pihak melakukan perilaku yang justru merugikan pihak lain, baik tanpa sadar atau bahkan dengan sengaja (Makarim, 2005). Jika melihat besarnya potensi ancaman siber yang tergambar dalam berbagai tindakan kejahatan di dunia maya. Apalagi resiko ancaman tersebut dapat menimpa siapapun baik saat penuh kesadaran ataupun ketika lengah.Beberapa tujuan ancaman siber yang seringkali terjadi, diantaranya (Magdalena, 2007):

1. Media sosial,
2. *Ecommerce*,
3. *Elearning*,
4. Kartu kredit,
5. Hak cipta, dan

6. Rahasia dagang.

Berdasarkan berbagai sumber penulis merangkum beberapa macam tindakan kejahatan di dunia maya, antara lain:

1. Penipuan,
2. Perusakan data,
3. Pembobolan informasi,
4. Akses tidak sah,
5. Pembajakan,
6. Penyadapan,
7. Pencurian data pribadi,
8. Penyebaran berita bohong,
9. Penyiaran ujaran kebencian,
10. Pornografi,
11. Pemerasan,
12. Kejahatan perbankan dan kartu kredit,
13. Pembajakan transaksi ekonomi, dan
14. Terorisme siber.

Apabila dilihat dari sisi pelaku kejahatan siber, maka dapat terbagi menjadi dua (Sulaiman, 2002):

1. Aktor internal, maksudnya adalah pelaku tersebut memiliki akses langsung terhadap korban. Hal ini ditunjukkan dengan upaya manipulasi, perubahan, dan modifikasi terhadap perangkat lunak maupun perangkat keras yang menghubungkan antara pelaku dan korban. Bentuk kejahatan yang dilakukan seringkali berkaitan dengan penipuan daring dan terorisme radikalisme. Biasanya hal ini sangat erat dengan kejahatan internet dengan jaringan yang sama oleh pelaku yang memiliki pengetahuan dan berpengalaman dalam bidang tertentu.

2. Aktor eksternal, maksudnya adalah pelaku dapat mengganggu dan merusak berbagai kegiatan di internet meskipun tidak memiliki jaringan yang sama dengan korban. Pelaku cenderung menggunakan sarana tulisan, suara, video, virus, dan *malware*. Tindakan kejahatan yang dilakukan kebanyakan dalam bentuk hoaks, ujaran kebencian, dan kejahatan siber. Meskipun tidak memiliki akses langsung, namun pelaku dapat melakukan tindakan yang dianggap merugikan nama baik, penyusupan, hingga pembobolan.

Merespon hal di atas Pemerintah Indonesia melakukan kerjasama dengan para penyedia jasa privat yang bernama *Indonesia Information Sharing and Analysis Center*. Forum kerjasama tersebut merupakan sarana berbagi informasi terkait ancaman, kerawanan, risiko, isu, penilaian, dan penanganan serangan siber pada bidang teknologi informasi. Meskipun cenderung berbasis sukarela, namun kerjasama ini memiliki banyak anggota perusahaan-perusahaan privat dan publik. Berdasarkan data Kominfo (2019) beberapa anggota dari forum ini, diantaranya:

1. PT Telkom,
2. PT Telekomunikasi Seluler,
3. PT Indosat,
4. PT XL Axiata,
5. PT Smart Telecom,
6. PT Xynexis International,
7. PT Aplikanusa Lintasarta,
8. PANDI,
9. PT Data Sinergitama Jaya (Elitery),
10. APJII,
11. PwC,
12. KPMG, dan

13. PT Sampoerna Telematika.

Kemudian, terdapat beberapa cara untuk mengatasi berbagai ancaman dalam penggunaan teknologi informasi, yakni: secara pendekatan budaya, pembaharuan teknologi, dan penegakan hukum.

Pertama, pendekatan budaya dapat dilakukan dengan membentuk kebiasaan sehat dalam penggunaan internet (Siagian, dkk, 2018). Publik dapat menggunakan dunia maya untuk berbagai hal yang bermanfaat positif, misalnya: berjualan, promosi, transaksi jasa, mencari literasi jurnal, dan lain-lain. Selain itu, penting untuk menangkal konten-konten negatif pada dunia maya dengan memperkuat literasi bagi masyarakat. Warganet didorong untuk lebih banyak membaca dan mencari tahu terlebih dahulu kebenaran informasi sebelum mempercayai dan menyebarluaskan. Masyarakat juga dapat melakukan pengecekan pada situs yang dimiliki pemerintah melalui Kementerian Komunikasi dan Informatika untuk mengecek keaslian informasi. Apabila komunitas siber telah tereduksi dan bisa membedakan informasi yang benar ataupun bohong, maka dapat mendorong secara perlahan pengguna internet untuk memerangi konten negatif. Pada akhirnya, kebiasaan yang baik dalam penggunaan internet akan membuat pemanfaatan ekosistem dunia maya yang baik sehingga memberikan manfaat bagi semua pihak.

Kedua, pembaharuan teknologi dapat dilakukan dengan mewajibkan setiap penyedia layanan di internet untuk meningkatkan keamanan secara rutin. Hal ini penting untuk melindungi jaringan, perangkat lunak, dan perangkat keras agar tidak disusupi, disadap, dan diakses secara ilegal. Penyedia jasa harus secara berkala memperbarui dan melindungi infrastruktur pada teknologi informasi dan komunikasi. Semakin luas cakupan layanan maka menyebabkan semakin besar pula pengguna yang berujung pada semakin tinggi resiko ancaman siber pada penyedia produk dan jasa tersebut. Jika sistem memiliki pertahanan dan

kemampuan keamanan yang kuat maka dapat menangkal berbagai ancaman sabotase, pembajakan, pencurian, dan perusakan data.

Ketiga, terkait penegakan hukum diperlukan adanya aturan yang memberikan kepastian dan penjelasan terhadap berbagai kegiatan di dunia maya. Merujuk pada hal tersebut memunculkan istilah hukum siber atau hukum dunia maya dalam rangka usaha perlindungan, pengawasan, dan penegakan hukum di dunia maya. Hukum siber ini dibutuhkan untuk memberikan kepastian hukum, perlindungan, dan sanksi terhadap hal-hal yang diperbolehkan dan dilarang dilakukan dalam penggunaan internet. Ada kecenderungan bahwa pengguna internet yang merasa memiliki hak, justru melanggar dan merugikan hak orang lain, baik dalam ide, ucapan, tindakan, dan tindakan lainnya selama menggunakan teknologi informasi. Sebaliknya terdapat oknum dan pihak tertentu yang sengaja untuk menciptakan hal buruk demi memenuhi kepentingan ekonomi dan politik tertentu.

Menindaklanjuti banyaknya ancaman yang terjadi di internet, Pemerintah Indonesia melakukan upaya pengakuan dan perlindungan siber terhadap masyarakat dengan ditunjukkan keberadaan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Ekonomi (UU ITE). Dalam UU ITE tersebut berisi penetapan, amanat, batasan, perlindungan, larangan, dan sanksi terhadap berbagai kegiatan yang berkaitan dengan pemanfaatan teknologi informasi dan komunikasi. UU ITE juga mengatur transaksi elektronik, perdagangan daring, dan pengakuan terhadap konten digital sebagai alat bukti yang sah dalam hukum.

Dalam aspek hukum siber yang tercantum dalam UU ITE telah secara jelas melindungi dan menegakkan hukum bagi siapapun yang memiliki, menyimpan, menyebarluaskan, dan melakukan tindakan apapun yang merugikan pihak lain dan melanggar hukum. Jika melihat realitas Indonesia yang memiliki jumlah pengguna internet terbesar yang

mencapai 202 juta orang menyebabkan semakin besar resiko serangan siber. Berkaca pada hal tersebut dalam UU ITE Pasal 27-34, Pasal 36-40 telah menjelaskan bentuk-bentuk pelanggaran hukum yang dilengkapi sanksi pidana, diantaranya: kerahasiaan data, serangan siber, dan pembobolan akses.

Keberadaan UU ITE merupakan salah satu dasar hukum terhadap perlindungan dan penegakan hukum kepada masyarakat Indonesia pengguna internet atau biasa disebut warganet (Harian Neraca ekonomi, 2019). Apalagi jika warganet tersebut mengalami kerugian akibat perbuatan orang lain di dunia maya, maka undang-undang ini dapat digunakan sebagai sarana pembelaan hak. Bahwa semua kegiatan yang dilakukan menggunakan internet yang menyebabkan kehilangan, kerusakan, dan kerugian terhadap warganet di Indonesia bisa menggunakan UU ITE sebagai alat hukum. Meskipun begitu, beberapa pihak menilai UU ITE dapat menjadi ‘pasal karet’ yang disalahgunakan atas dasar pencemaran nama baik terhadap hal apapun di internet.

Berdasarkan rilis Direktorat Jenderal Perundang-undangan Kementerian Hukum dan HAM (2019), penulis menghimpun setidaknya terdapat dua puluh hal yang dijamin dalam UU ITE, seperti:

1. Kerahasiaan
2. Perlindungan data
3. Pengamanan transaksi ekonomi
4. Tanda tangan elektronik
5. Rahasia dagang
6. Hak atas Kekayaan Intelektual (HaKI)
7. Promosi daring
8. Alat bukti elektronik
9. Legalitas jasa daring
10. Tanggung jawab jasa daring
11. Perlindungan transaksi keuangan dan investasi

12. Proteksi atas penghilangan informasi
13. Penyelesaian sengketa
14. Larangan penyebarluasan berita bohong
15. Larangan penghinaan
16. Larangan perjudian
17. Larangan kegiatan prostitusi dan asusila
18. Larangan pemerasan
19. Larangan pengancamanan dengan kekerasan
20. Larangan penipuan daring.

Berikutnya, terdapat juga Kitab Undang-Undang Hukum Pidana (KUHP) dan Kitab Undang-Undang Hukum Perdata (KUHPer). Kedua aturan hukum tersebut telah menjelaskan perintah, larangan, dan hukuman kepada setiap pihak dan lembaga yang merugikan pihak lain, terutama apabila terjadi dalam dunia maya. Semua tindakan yang dianggap mengganggu, merusak, dan merugikan orang lain dalam bentuk apapun dapat dikenakan dalam aturan hukum KUHP dan KUHPer. Ini dapat menunjukkan bahwa perlindungan dan penegakan hukum siber tidak hanya berfokus pada UU ITE, akan tetapi juga berhubungan erat dengan aturan hukum lainnya dengan mempertimbangkan kemajuan teknologi.(Ersya, 2017).

Namun, terdapat kendala apabila terjadi serangan siber yang dilakukan oleh aktor berasal dari luar negeri akibat pelaku berada di luar wilayah hukum Indonesia. Cenderung sulit apabila akan dilakukan penegakan hukum sementara pelaku bukan warga negara dan tidak berdomisili di Indonesia. Aturan UU ITE, KUHP, dan KUHPer memerlukan proses dan waktu yang lama untuk dapat melakukan proses peradilan. Dibutuhkan adanya kerjasama dan aturan bersama terkait perlindungan, pengawasan, dan penegakan hukum lintas negara terhadap aktor-aktor yang menyebabkan kerugian terhadap warganet Indonesia.

Pemerintah Indonesia bisa menggunakan jalur diplomasi dan penegakan hukum dengan bekerjasama negara sahabat ataupun melaporkan kepada Interpol.

Usaha Diplomasi Siber Indonesia Terhadap Global

Terkait perlindungan terhadap serangan siber, dunia internasional telah memiliki aturan bersama bernama *Paris Call for Trust and Security in Cyberspace*. Aturan ini telah ditandatangani oleh 51 negara dunia termasuk diantaranya negara-negara maju di Eropa. Perjanjian internasional tersebut bertujuan untuk menangkal serangan dan perang siber. Melalui perjanjian tersebut telah mengatur bahwa seluruh infrastruktur dan fasilitas internet tidak disalahgunakan menjadi sarana serangan siber (CNN, 2019). Selain itu, dengan konvensi ini dapat mencegah agar tidak terjadi perang siber yang berujung pada konflik dan perang di dunia nyata. Akan tetapi, keberadaan isu siber belum sepenuhnya memiliki pemahaman yang sama karena cenderung dikuasai oleh pihak militer untuk pertahanan diri dan pembalasan serangan (CNN Indonesia, 2019).

Lebih lanjut, terdapat organisasi internasional yang bertugas untuk membahas kerjasama global terkait keamanan siber bernama *International Telecommunication Union* (ITU). ITU berdiri pada tahun 2003 yang merupakan tindak lanjut dari Sidang Umum PBB tahun 2001 dalam rangka mengatasi serangan siber secara bersama-sama. ITU menjadi garda terdepan dalam mempromosikan nilai dan standar bersama dalam dunia maya agar dapat dimanfaatkan secara positif. Meskipun menjadi lembaga siber tertinggi dunia, tetapi ITU memiliki kekurangan terkait tidak dimilikinya kewenangan untuk memberikan penindakan hukum bagi masing-masing negara. Akibatnya setiap negara cenderung lebih banyak melaksanakan perlindungan atas serangan dan perang siber

sesuai dengan kepentingannya masing-masing. Selain itu, masing-masing negara kemudian membuat kebijakan sesuai inisiatif dan kebutuhan nasionalnya. Terkait penegakan hukum, kebanyakan negara lebih memilih untuk bekerja sama dengan Interpol untuk dapat menangkap pelaku serangan siber di negara lain. (Parestri, 2016). Selain ITU, terdapat juga kerjasama internasional terkait ancaman siber, yaitu: *International Multilateral Partnership Against Cyber Threats* (IMPACT). IMPACT berdiri tahun 2011 yang juga bekerjasama dengan ITU (Kittichaisaree, 2017).

Adanya pertentangan terkait pemahaman dalam keamanan siber pada setiap negara di dunia internasional diduga terjadi akibat perkembangan politik global dan perbedaan kepentingan nasional. Hal tersebut justru menjadi hambatan untuk membuat rezim perlindungan dan tata kelola keamanan siber. Terdapat sejumlah faktor yang menyebabkan hambatan tersebut, diantaranya (Cahyadi, 2017):

1. Perbedaan norma dan nilai yang dipahami setiap negara
2. Perbedaan kepentingan antara negara maju dan berkembang
3. Perbedaan cara pandang dalam pertahanan siber
4. Belum adanya perjanjian yang mengikat sepenuhnya setiap negara
5. Setiap negara berusaha menguasai dunia siber.

Merujuk pada dinamika realitas dalam dunia internasional di atas maka diperlukan adanya diplomasi siber yang harus dilakukan oleh Pemerintah Indonesia. Kenyataan bahwa semakin meluasnya penggunaan media sosial dan transaksi keuangan di dunia maya menunjukkan potensi dan resiko yang besar. Pemerintah perlu memperjuangkan perlindungan keamanan siber terhadap seluruh aktivitas di internet demi kemaslahatan masyarakat Indonesia. Pemerintah Indonesia juga harus memetakan ancaman dan segera melakukan upaya proteksi berdasarkan analisa mendalam agar bisa memperoleh kebijakan yang tepat. Pemerintah dapat

melakukan diplomasi terhadap negara lain yang warganya menjadi pelaku atau asal serangan siber. Apabila pemerintah terlambat mengatasi perlindungan dan penegakan hukum pada dunia maya maka akan berujung pada kerugian ekonomi, sosial, dan politik yang sangat besar karena berdampak pada terjadinya konflik dan korban jiwa di dunia nyata.

Merespons hal tersebut, Indonesia telah berhasil menjadi salah satu inisiator dalam deklarasi bersama bernama *ASEAN Declaration to Prevent and Combat Cybercrime* pada 2017. Kesepakatan tersebut dapat menjadi dasar rujukan dan bentuk pemahaman bersama terhadap ancaman keamanan siber. Pemerintah Indonesia secara aktif juga mendorong kerjasama lintas negara pada level bilateral, multilateral, dan internasional yang mendukung penggunaan internet secara bijaksana (Media Indonesia, 2019).

Menindaklanjuti deklarasi perlindungan siber di kawasan Asia Tenggara di atas terdapat *Computer Emergency Response Teams* (CERTs), *Telecommunication Ministerial Meeting* (TELMIN) dan *ASEAN Digital Ministerial Meeting* (ADMIN). CERTSs adalah forum yang membahas permasalahan siber dan upaya menghadapi ancaman serangan siber (Kittichaisaree, 2017). Sementara TELMIN merupakan forum negosiasi di kawasan yang kemudian berkembang menjadi ADMIN atas masukan Indonesia untuk membahas isu siber dan digital sejak tahun 2019. Melalui TELMIN dan ADMIN, Indonesia berkontribusi dalam berbagai pertemuan untuk lebih membahas perlindungan digital menjadi siber yang lebih luas. Sementara beberapa lembaga Pemerintah Indonesia yang melakukan diplomasi siber, diantaranya: Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan (Kemenko Polhukam), Kementerian Luar Negeri (Kemlu), Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informasi (Kemenkominfo), Kementerian Pertahanan (Kemhan), dan Tentara Nasional Indonesia (TNI) (Chotimah dkk, 2019).

Salah satu bentuk diplomasi yang dilakukan BSSN adalah dengan melakukan kemitraan terhadap berbagai negara dunia, sepert: Amerika Serikat, Tiongkok, Rusia, Inggris, Belanda, dan Australia (BSSN, 2019). Kerjasama yang dilakukan oleh BSSN tersebut terkait perlindungan dan terorisme siber. Diplomasi antara BSSN dan mitra di Amerika Serikat, Tiongkok, dan Rusia dapat menjadi upaya pemetaan dan sarana mitigasi mengingat ketiga negara tersebut merupakan negara-negara yang menjadi tujuan serangan siber terbesar di dunia. Melalui berbagai kerjasama dan diplomasi tersebut dapat menjembatani kepentingan Indonesia guna melindungi dan melakukan penegakan hukum siber di dunia maya.

Indonesia juga secara aktif mengadakan dan berpartisipasi dalam berbagai pertemuan internasional dalam diskusi publik secara global, seperti: membuat *Policy Planning Consultation* (PCC) di Jenewa pada 2017, mengikuti *5th Annual Cyber Intelligence Asia* di Malaysia tahun 2017, dan terlibat dalam *Open-Ended Working Group (OEWG) on International Information Security* pada 2019 (Kemlu, 2018).

Berdasarkan berbagai penjelasan di atas dapat dipahami bahwa perkembangan teknologi informasi dan komunikasi di Indonesia telah memunculkan bermacam manfaat dan ancaman. Pemerintah Indonesia telah membuat aturan UU ITE Tahun 2008 dan mendorong pemanfaatan internet secara bijaksana dan positif melalui berbagai pendekatan. Selanjutnya Pemerintah Indonesia juga melakukan upaya diplomasi siber melalui beberapa kementerian terkait terhadap negara-negara lain, baik secara bilateral, regional, multilateral, dan internasional. Akan tetapi semuanya bergantung pada setiap pengguna internet agar selalu waspada dan berhati-hati dalam menggunakan dunia maya agar terhindar dari ancaman kejahatan siber.

Daftar Referensi

Bisnis.com. *Ancaman Siber Indonesia Terbanyak Kelima Se-Asia Pasifik*. https://teknologi.bisnis.com/read/20190306/84/896967/ancaman-siber-di-indonesia-terbanyak-kelima-se-asia-pasifik. diakses pada 24 Juni 2021.

Badan Siber dan Sandi Negara. *Building a National Soft-Power on Cyber Space Through Cyber Diplomacy*. https://bssn.go.id/building-a-national-soft-power-on-cyber-space-through-cyber-diplomacy/. diakses pada 24 Juni 2021.

Cahyadi, Indra. (2016) Cyber Governance and Threat of National Sovereignty. *Politica*. No. 7, Vol. 2.

Chotimah, Hidayat Chusnul; Iswardhana, Muhammad Ridha; Pratiwi Tiffany Setyo. (2019). Penerapan Military Confidence Building Measures dalam Menjaga Ketahanan Nasional Indonesia di Ruang Siber. *Jurnal Ketahanan Nasional*. Vol. 25. No. 3.

CNN Indonesia. (2019). *51 Negara Dukung turan Keamanan Siber Global*. https://www.cnnindonesia.com/teknologi/20181113075756-185-346044/51-negara-dukung-aturan-keamanan-dunia-siber-global. diakses pada 25 Juni 2021.

Danuri, Muhammad dan Suharnawi. (2017). Tren Cyber Crime dan Teknologi Informasi di Indonesia. *Infokam*, No.2.

Direktorat Jenderal Peraturan Perundang-Undangan. *Hukum Teknologi Informasi*. http://ditjenpp.kemenkumham.go.id/hukum-teknologi/668-dinamika-konvergensi-hukum-telematika-dalam-sistem-hukum-nasional.html. diakses pada 24 Juni 2021.

Ersya, Muhammad Prima. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education Edisi 2017*.

Fahmi, Novrizal. (2018). Melawan Aksi Terorisme di Media Sosial: Penggunaan Tagar #KamiTidakTakut di Twitter. *Jurnal Komunika*. Vo.1. No.1.

Febriansyah, Ferry Irawan & Purwinatro, Halda Septiana. (2020). Pertanggungjawaban Pidana bagi Pelaku Ujaran Kebencian di Media Sosial. *Jurnal Penelitian Hukum De Jure*. Vol.20. No.2.

Harian Ekonomi Neraca. (2019). *Menyikapi Positif Perkembangan Dunia Cyber*. http://www.neraca.co.id/article/87868/menyikapi-positif-perkembangan-dunia-cyber. diakses 24 Juni 2021.

Infokomputer. (2021). *Pengguna Internet Indonesia Terbesar ke-4 di Dunia Ini Tantangannya*. https://infokomputer.grid.id/read/122756150/pengguna-internet-indonesia-terbesar-ke-4-di-dunia-ini-tantangannya. diakses 24 Juni 2021.

Jawa Pos. (2019). *Kaleidoskop 2019: Karena Berita Hoax Kerusuhan Wamena Pecah*. https://www.jawapos.com/nasional/28/12/2019/kaleidoskop-2019-karena-berita-hoax-kerusuhan-wamena-pecah/. diakses 24 Juni 2021.

Juditha, Christiany. (2018). Interaksi Komunikasi Hoax di Media Sosial serta Antisipasinya Hoax Communication Interactivity in Social Media and Anticipation. *Jurnal Pekommas*. Vol. 3. No. 1.

Junaedi, Fajar. (2010). Relasi Terorisme dan Media. *Jurnal ASPIKOM*. Vo.1. No.1.

Kementerian Komunikasi dan Informasi. (2018). *Tingkatkan Koordinasi Proteksi Keamanan Siber di Indonesia*. https://kominfo.go.id/content/detail/14605/ciip-id-summit-2018-tingkatkankoordinasi-proteksi-keamanan-siberindonesia/0/sorotan_media. diakses pada 25 Juni 2021.

Kementerian Luar Negeri Republik Indonesia. (2018). *LAKIP Kemenlu*.

Kittichaisaree, Kriangsak. (2017). *Public International Law of Cyberspace*. Switzerland: Springer International Publishing.

Kompas.com. (2020). *Akankah Work From Home Jadi Tren Setelah Pandemi Covid-19 Berakhir?*.https://www.kompas.com/tren/read/2020/04/21/070400465/akankah-work-from-home-jadi-tren-setelah-pandemi-covid-19-berakhir-?page=all. diakses pada 25 Juni 2021.

Kompas.com. (2021). *Jumlah Pengguna Internet Indonesia 2021 Tembus 202 Juta*. https://tekno.kompas.com/read/2021/02/23/16100057/jumlah-pengguna-internet-indonesia-2021-tembus-202-juta. diakses pada 25 Juni 2021.

Kusumasari, Dita & Arfianto, S. (2020). Makna Teks Ujaran Kebencian Pada Media Sosial. *Jurnal Komunikasi*. Vol. 12. No. 1.

Liputan6.com. (2019). *50 Juta Ancaman Siber Diblokir di Indonesia Sepanjang 2018*. https://www.liputan6.com/tekno/read/3947074/50-juta-ancaman-siber-diblokir-di-indonesia-sepanjang-2018?utm_expid=.9Z4i5ypGQeGiS7w9arwTvQ.0&utm_referrer=https%3A%2F%2Fwww.google.com%2F. diakses pada 25 Juni 2021.

Magdalena, Merry dan Setyadi, Maswigrantoro R. (2007). *Cyberlaw, Tidak Perlu Takut*. Yogyakarta: Penerbit Andi.

Makarim, Edmon. (2005). *Pengantar Hukum Telematika – Suatu Kompilasi Kajian*. Yogyakarta: Badan Penerbit FH UII.

Media Indonesia. (2019). *Merajut Diplomasi Siber Indonesia*. https://mediaindonesia.com/read/detail/199360-merajut-diplomasi-siber-indonesia. diakses pada 25 Juni 2021.

Ningrum, Dian Junita; Suryadi; Wardhana, Dian E.C. (2018). Kajian Ujaran Kebencian di Media. *Jurnal Ilmiah Korpus*. Vol.2. No.3.

Nuruzzaman, Muhammad. (2018). Terorisme Dan Media Sosialsisi Gelap Berkembangnya Teknologi Informasi Komunikasi. *Jurnal Ilmiah Indonesia Syntax Literate*. Vo. 3. No.9.

Parestri, Awinditya. (2016). Negara Liliput dalam Persoalan Digital: Upaya-upaya Swiss Menghadapi Ancaman Keamanan Siber. *Jurnal Analisis Hubungan Internasional*. Vol. 5. No. 2.

Republika. (2021). *Kominfo: Pengguna Internet Indonesia Terbesar ke-4 di Dunia*. https://www.republika.co.id/berita/qv56gb335/kominfo-pengguna-internet-indonesia-terbesar-ke4-di-dunia. diakses pada 25 juni 2021.

Samudra, Anton Hendrik. (2019). Modus Operandi dan Problematika Penanggulangan Tindak Pidana Penipuan Daring. *Mimbar Hukum*. Vol. 31. No.1.

Siagian, Lauder; Budiarto, Arief, Simatupang. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. *Jurnal Prodi Perang Asimetris*. Vol. 4. No. 3

Suara.com. (2014). *Membongkar Kecanggihan Pasukan Hacker Korea Utara*. https://www.suara.com/tekno/2014/12/24/073200/membongkar-kecanggihan-pasukan-hacker-korea-utara. diakses pada 25 juni 2021.

Sulaiman, Robintan. (2002). *Cyber Crimes: Perspektif E-Commerce Crime*. Tangerang: Pusat Bisnis Fakultas Hukum Universitas Pelita Harapan.

Sumenge, Melisa Monica.(2013). Penipuan Menggunakan Media Internet Berupa Jual Beli. *Lex Crimen*. Vol.II. No.4

TEKNOLOGI MOBILE

Suyud Widiono, S.Pd., M.Kom

Beliau berprofesi sebagai Dosen dan juga seorang Praktisi IT. Dengan sertifikasi MTCNA (Mikrotik Certified Network Associate) Certificate Trainer, Senior Web& Mobile Programmer, Computer Network Engineer, Cloud & On-Promise Server Administrator, IT Consultant.

Tren Teknologi Mobile

Peradaban manusia terus berkembang maju dan baru, seiring pula dengan perkembangan tren teknologi yang juga terus berkembang semakin canggih, bekerja secara otomatis, dan berkemampuan yang futuristik. Beberapa tren teknologi dibawah ini merupakan contoh teknologi yang sedang berkembang di tahun 2020, yaitu:

A. Teknologi Jaringan Komunikasi Data Cellular 5G

Teknologi Jaringan Cellular 5G berbeda dengan Jaringan Wireless Fidelity (WiFi) 5G. Jaringan Cellular 5G merupakan teknologi *Fifth Generation* (generasi kelima) dari jaringan komunikasi data cellular, sedangkan Jaringan WiFi 5G merupakan kependekan dari "5 Ghz" yaitu salah satu dari dua pita frekuensi yang digunakan oleh WiFi, selain 5 Ghz, pita frekuensi lainnya adalah 2,4 Ghz, yang keduanya menggunakan standar Protokol Jaringan Wireless (WiFi) dari *Institute of Electrical and Electronics Engineers* (IEEE) 802.11n.

Teknologi Jaringan 5G ini menggunakan gelombang radio milimeter yang 10-100 kali lebih cepat bisa mencapai 800 Gbps dan lebih kuat serta memiliki latensi lebih rendah (latency = interval antara pengirim dan penerima) daripada 4G LTE *(Long Term Evolution)* dan WiFi. Selain kelebihan tersebut, jaringan 5G juga akan menjadi penunjang pentingnya bagi perangkat mobil otonom, drone serta *Internet of Things* (IoT) yang berguna untuk pelacakan logistik, *smart city*, *smart building*, agrikultur serta Industry 4.0.

Pengembangan jaringan 5G ini memiliki target antara lain adalah;

1. Rata rata kecepatan data lebih tinggi

   Jaringan 5G secara signifikan lebih cepat daripada jaringan sebelumnya yaitu jaringan 4G. Dengan menghantarkan 20 Gigabit per second pada titik tertingginya dan 100 Megabit per second pada rata-ratanya.
2. Mengurangi latency (interval antara pengirim dan penerima)

   Jaringan 5G secara signifikan mengurangi tingkat latency untuk mengantarkan secara instant, real-time dari perangkat pengirim ke perangkat penerima.
3. Menghemat energy
4. Mengurangi biaya
5. Menambah kapasitas system

   Jaringan 5G mampu men-support 100 kali lipat kapasitas traffic dan efisiensi jaringan.
6. Konektivitas perangkat secara massive baik *smart phone* maupun *smart device*.

B. Smart Home

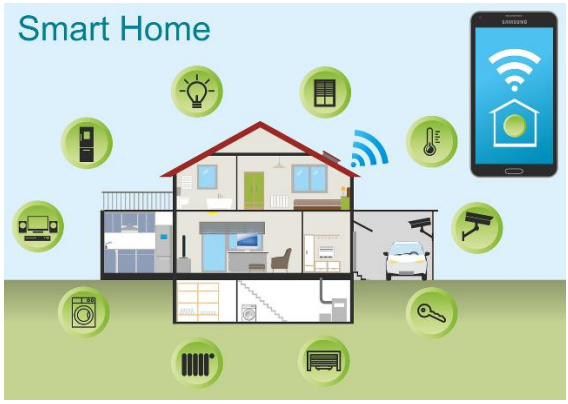
Smart home atau yang bisa juga disebut dengan rumah pintar adalah rumah yang dipenuhi oleh peralatan-peralatan pintar yang dapat bekerja secara otomatis. Misalnya smart toilet, robot vacuum cleaner,

pembuka garasi otomatis, hingga tempat tidur pintar, sehingga menjadikan segala sesuatu yang ada di dalam rumah terintegrasi dalam sistem teknologi canggih seperti tersambung dengan aplikasi virtual assistant yang ada di smartphone atau komputer, seperti Google Assistant atau Google Smart Home, Alexa, Watson, dan Siri.

www.qword.com

Meski belum menjadi tren di Indonesia, namun smart home akan semakin popular dan berkembang. Di negara maju seperti Amerika dan Jepang, sistem ini sudah banyak digunakan dan terbukti membantu mempersingkat waktu dalam mengelola rumah. Selain itu, smart home sering digunakan untuk meningkatkan keamanan rumah yang bisa dipantau jarak jauh secara mobile dengan cara yang mudah.

Membuat rumah biasa jenis apapun menjadi Smart Home, cukup mengubah beberapa hal yang ada di rumah menjadi *technology friendly*. Pertama adalah mengganti beberapa saklar yang nantinya akan menjadi sarana penghubung pada perangkat elektronik canggih di rumah, lalu menyiapkan jaringan internet yang akan menjadi jaringan utama IoT *(Internet of Things)* agar semua proses peralihan menuju rumah pintar bisa berjalan lancar. Namun ketika akan baru membangun rumah, sebaiknya langsung dipersiapkan jaringan listrik dan jaringan internet yang akan menunjang penggunaan berbagai perangkat elektronik berbasis rumah pintar, sehingga pengertian Smart Home yang bagi sebagian orang mungkin masih terlalu *high class* sekarang semua kalangan bisa mengimplementasikan rumah pintar ini.



www.qword.com

Cara Kerja Smart Home melalui satu alat transmitter yang memancar melalui jaringan internet WiFi sebagai pusat kendali. Dari peralatan transmitter yang dilengkapi dengan sensor keadaan rumah ini akan dikendalikan semua jenis peralatan elektronik yang ada di rumah dengan remote digital. Remote digital inilah yang di sinkronisasikan dengan aplikasi di perangkat ponsel atau komputer.

C. *Artificial intelligent* semakin meluas

Teknologi *Artificial Intelligence* (AI) sudah banyak diimplementasikan pada kamera smartphone yang dapat digunakan untuk meningkatkan kualitas kamera secara lebih maksimal. Adanya Teknologi AI di kamera smartphone juga dapat membuat pengaturan gambar berjalan secara otomatis. Dengan AI, antarmuka kamera smartphone dapat mendeteksi objek dalam frame foto secara otomatis, baik itu foto pemandangan yang diambil secara *landscape* atau foto diri dengan mode *portrait* dengan detil yang lebih tajam, lalu memaksimalkan setting kamera sehingga menghasilkan hasil foto yang maksimal kualitasnya. AI juga dapat mengenal fitur wajah dengan teknologi *facial recognition* dan memberikan efek *beauty* yang disesuaikan dengan kontur muka pengguna.

Selain itu Teknologi AI pada smartphone juga digunnakan untuk menerapkan *voice assistant* yang diterapkan pada aplikasi penerjemah yang mampu menerjemahkan teks, gambar, video, maupun suara secara real-time.

Teknologi AI didesain untuk belajar dan beradaptasi tiap kali digunakan. AI dalam smartphone akan mempelajari pola pemakaian oleh si pengguna, kemudian mengaplikasikannya dalam penggunaan sehari-hari.

Penerapan teknologi AI pada *asisten digital* yang diterapkan pada *smart device* dan smartphone *flagship* dapat menerima perintah berupa suara. Asisten digital tersebut mampu merespon suara untuk melakukan beberapa tugas seperti menjawab pesan singkat, memutarkan lagu, atau membacakan isi berita.

D. Teknologi automasi

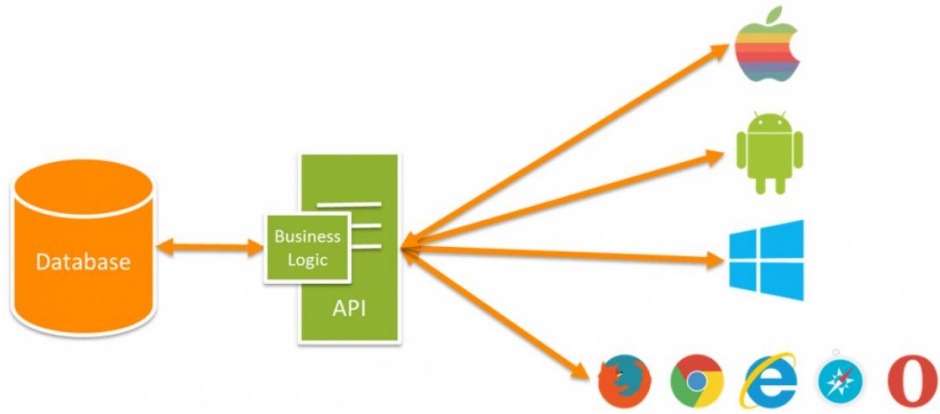
Gerakan Industri 4.0 mendorong meningkatkan perkembangan teknologi otomatisasi, yang menggerakkan transformasi digital untuk semakin menuntut modernitas.

Automasi berasal dari bahasa Yunani, “Automotos” yang membawa maksud bergerak sendiri *(self-moving)* dan Bahasa Latin “Ion” yang memberi maksud tetap *(a state)*. Kata automasi muncul pada tahun 1936 oleh D.S Harder dan automasi berkembang sejak tahun 1952.

Pengembangan Teknologi Mobile

Untuk mengembangkan teknologi mobile dalam bentuk aplikasi/perangkat lunak, aplikasi mobile terutama yang berkaitan dengan IoT *(Internet of Things)* pasti akan memanfaatkan Konsep API *(Application Programming Interface)*, yang merupakan perantara software

(perangkat lunak) yang memungkinkan 2 (dua) atau lebih aplikasi untuk saling berinteraksi meskipun berbeda platform Sistem Operasi.



https://www.codepolitan.com/

Fungsi API untuk menyediakan function dan perintah untuk menggantikan bahasa yang digunakan *system calls interface* pada Sistem Operasi dengan bahasa yang lebih terstruktur dan lebih mudah dipahami oleh programmer. *System call interface* berfungsi sebagai penghubung API dengan *system call* yang dimengerti oleh sistem operasi.

Dalam konsep API yang menggunakan protocol jaringan TCP/IP dan protocol aplikasi HTTP, muncul 2 (dua) konsep API yang disebut Web API dan Web Service. Perbedaan Web API dan Web Service adalah:

Semua web service digunakan sebagai API, tapi tidak semua API digunakan sebagai web service.

1. Web service digunakan untuk interaksi dua perangkat atau aplikasi melalui jaringan. Sedangkan API digunakan interaksi antara dua aplikasi berbeda baik dengan ataupun tanpa jaringan.
2. Web service hanya menggunakan 3 style yaitu SOAP, REST, atau XML-RPC untuk berkomunikasi sedangkan API dapat menggunakan style apapun.

3. Web service selalu membutuhkan jaringan untuk pengoperasiannya sedangkan API tidak selalu memerlukan jaringan untuk operasinya.

API dapat diklasifikasikan menjadi 3 (tiga) kategori yaitu:

1. Ownership web API

Terdapat 4 (empat) macam API Utama dalam jenis ini, yaitu:

a. Open API

API yang tersedia untuk umum dan digunakan seperti API oauth dari Google dan tidak ada batasan untuk menggunakannya.

b. Partner API

API dimana harus ada hak atau lisensi khusus untuk mengakses API jenis ini.

c. Internal API

API yang dikembangkan oleh perusahaan untuk digunakan pada sistem internal.

d. Composite API

API ini adalah berupa urutan task atau tugas yang berjalan secara sinkron (bersamaan) sebagai hasil dari sebuah eksekusi.

2. Communication level API

API dalam kategori ini, terdapat 2 (dua) macam API yaitu:

a. High Level API

API dalam bentuk REST untuk programmer yang menginginkan pengukuran program dengan hanya menggunakan event preset PAPI pada komponen CPU.

b. Low Level API

API yang memiliki tingkat abstraksi yang lebih rendah sehingga lebih rinci, yang memungkinkan programmer untuk memanipulasi fungsi yang terdapat dalam modul aplikasi atau dalam hardware pada tingkat

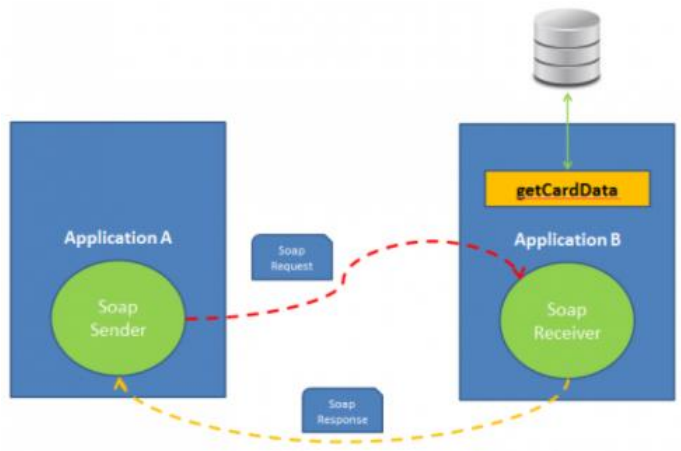
granular dan sering digunakan dalam mengirim video atau umpan media secara real-time.

3. Web service API

Klasifikasi API jenis ini dilakukan pada jenis komunikasi dan pendekatan behavior atau perilaku yang digunakan dalam membangun API, yaitu:

a. SOAP (Simple Object Access Protocol)

API ini telah ada sejak akhir 1990-an dan menggunakan XML untuk mentransfer data. Ini membutuhkan aturan ketat dan keamanan tingkat lanjut yang membutuhkan lebih banyak bandwidth.



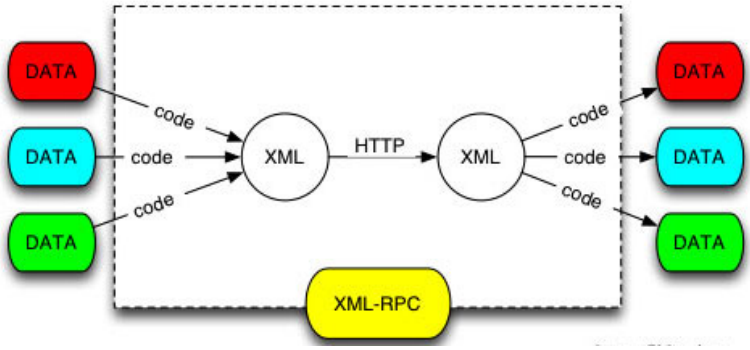
https://techarea.co.id/

Protokol ini tidak memiliki kemampuan untuk melakukan cache, memiliki komunikasi yang ketat dan membutuhkan setiap informasi tentang interaksi sebelum panggilan apa pun dianggap diproses.

b. XML-RPC (eXtensible Markup Language – Remote Procedure Call)

XMLRPC adalah akronim dari eXtensible Markup Language – Remote Procedure Call. Sebuah spesifikasi XML yang menjelaskan mengenai mekanisme pemanggilan prosedur jarak jauh dengan menggunakan XML. XMLRPC adalah salah satu bentuk webservice yang disederhanakan dari standar yang konvensional. Dua sistem yang benar-benar terpisah dan berbeda platform serta lingkungan bisa saling berkomunikasi lewat sarana file XML.

Protokol komunikasi yang digunakan adalah protokol HTTP. Request yang dikirim lewat HTTP harus menggunakan method POST. Prosedur yang akan dipanggil beserta parameternya dibungkus dalam file XML dalam spesifikasi XMLRPC dan lebih sederhana dibanding konsep setelahnya yaitu SOAP, UDDI dan WSDL. Return value sebelum dikirim akan dibungkus dulu dalam bentuk XML dan ditransfer diatas lalu lintas protokol HTTP di internet.



https://www.codepolitan.com/

c. JSON-RPC

JSON-RPC merupakan sebuah protokol yang memungkinan untuk melakukan pemanggilan method secara remote ke program lain yang

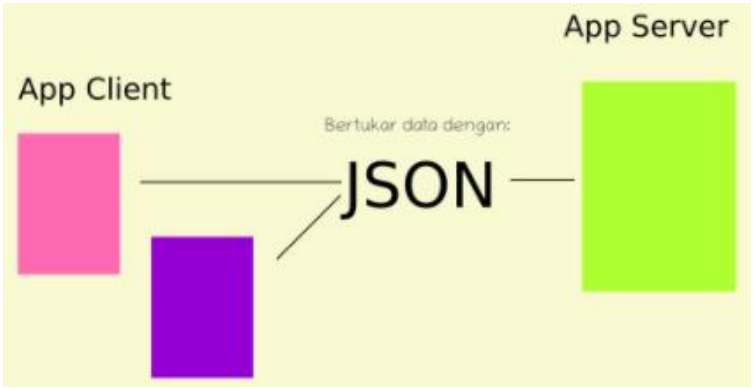
berada di alamat yang berbeda dengan menggunakan JSON sebagai pembungkus pesannya.

JSON-RPC ini memliki 2 versi, yaitu versi 1.0 dan 2.0. Yang membedakan antara keduanya adalah pada pengaturan format pesan saat pertukaran data.

Type data yang ditransferkan dalam bentuk sebuah object yang di serialisasi dengan menggunakan JSON. Permintaan bisa langsung ditujukan kepada method yang telah di sediakan oleh server. Dan dalam sebuah pengiriman paket tersebut memiliki 3 (tiga) properti, yaitu, pada pesan pengiriman:

- **Method** - isi data ini bertujuan untuk menentukan method mana yang diminta oleh client untuk di jalankan di server.
- **Params** - merupakan sebuah object array yang berisi parameter dan value untuk kebutuhan method yang akan di panggil di server.
- **Id** - berisi type sembarang yang bertujuan untuk pengecheckan apakah yang request nanti sama dengan yang di kembalikan.

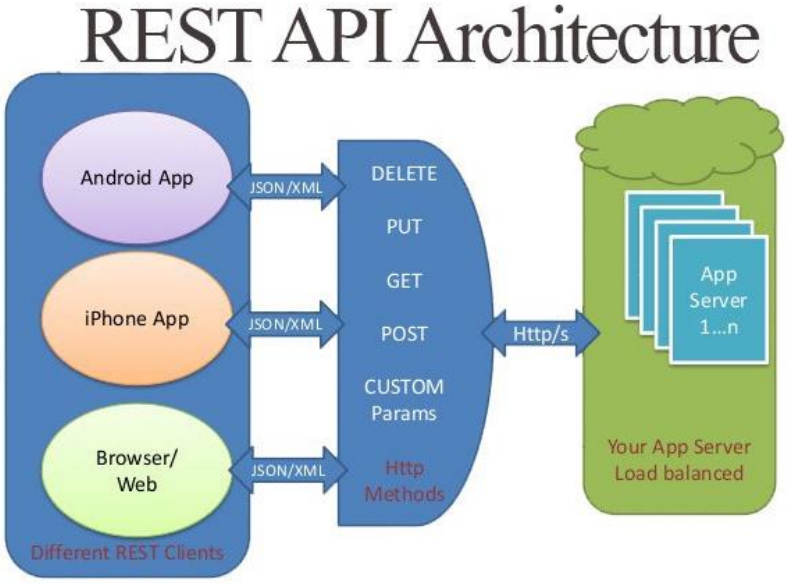
  Pada pesan response dari server:
- **Result** - merupakan data keluaran dari method yang di panggil di server.
- **Error** - merupakan pengembilan dari server jika terjadi error saat menjalankan service rpc. Jika tidak ada, maka akan dikembalikan null
- **Id** - berisi data dari id request yang di minta oleh requestor



https://techarea.co.id/

d. REST (RESTful) API.

REST *(Representional State Transfer)* adalah suatu arsitektur metode komunikasi yang menggunakan protokol HTTP untuk pertukaran data dan metode ini sering diterapkan dalam pengembangan aplikasi. Dimana tujuannya adalah untuk menjadikan sistem yang memiliki performa yang baik, cepat dan mudah untuk di kembangkan (scale) terutama dalam pertukaran dan komunikasi data..



https://techarea.co.id/

REST memanfaatkan empat metode di protocol HTTP, yaitu:

- GET, berfungsi untuk membaca data/resource dari REST server
- POST, berfungsi untuk membuat sebuah data/resource baru di REST server
- PUT, berfungsi untuk memperbaharui data/resource di REST server
- DELETE, berfungsi untuk menghapus data/resource dari REST serve.

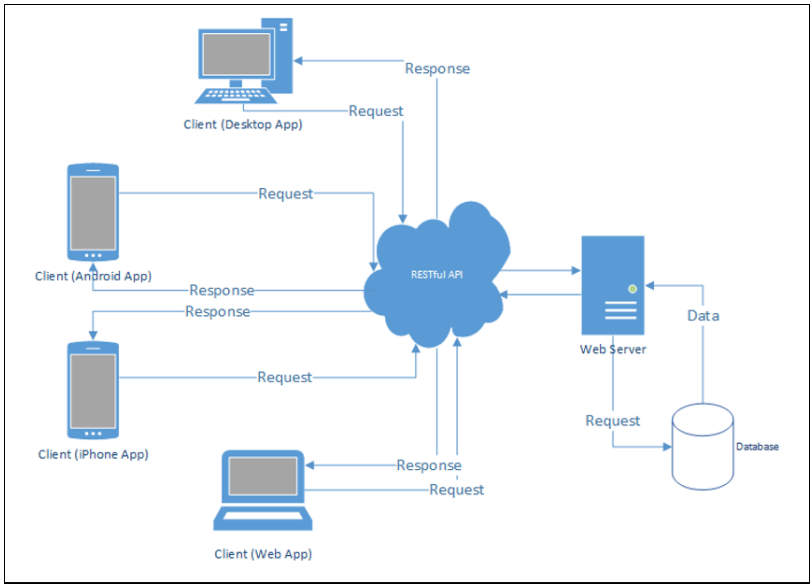
Ada lagi method lainnya yang dapat digunakan, yaitu:

- CONNECT, membuat terowongan ke server diidentifikasi sumber daya target.
- TRACE, pengujian loop-kembali pesan di sepanjang jalur ke sumber daya target.
- PATCH, digunakan untuk menerapkan modifikasi parsial ke sumber daya.
- OPTIONS, untuk mendapatkan operasi yang disupport REST server.

4. Implementasi REST (RESTful) API

Gambaran dalam implementasi REST API, dapat di gambarkan sebagai berikut:

Terdapat beberapa platform aplikasi di sisi klien, baik Desktop, Mobile maupun web browser. Komunikasi dari client ke server dilayani menggunakan protocol HTTP dan format data baik client maupun server menggunakan JSON.



http://mfikri.com/

a. Design EndPoint RESTful API

Sebelum membuat RESTful API, perlu didefinisikan EndPoint dari RESTful API yang akan dibuat. EndPoint merupakan routes dari API yang akan dibuat. RESTful API menggunakan HTTP verbs: GET, POST, PUT, dan DELETE. GET untuk mendapatkan data dari server atau lebih dikenal dengan istilah READ, POST untuk meng-CREATE new data, PUT untuk UPDATE data, dan DELETE untuk menghapus data, atau lebih dikenal dengan istilah CRUD (Create-Read-Update-Delete). Pada kesempatan kali ini, akan disharingkan bagaimana membuat RESTful API sederhana untuk membuat data baru ke server (POST) dari suatu table di database yaitu table users. Berikut rancangan EndPoint dari RESTful API yang dibuat:

Method	EndPoint	Description
POST	/auth/register	Create New User {first_name, last_name, email, password}
GET	/auth/ login	View Respon
PUT	/auth/{id}	-
DELETE	/auth/{id}	-

b. Instalasi dan pemanfaatan framework web

Framework yang digunakan pada kesempatan ini adalah Codeigniter 4. Dokumentasi resmi codeigniter, CI4 membutuhkan spesifikasi PHP >= 7.2. Adapun kita perlu memastikan beberapa server requirement yang dibutuhkan saat melakukan installasi Codeigniter 4, di antaranya: intl extension, mbstring extension, php-json, php-mysqlnd, dan php-xml. Untuk pengguna windows bisa langsung membuka file php.ini kemudian uncomment untuk extension di atas. Contoh di xampp:

```
;extension=intl
// ubah menjadi
extension=intl
;extension=mbstring
// ubah menjadi
extension=mbstring
```

Begitu juga dengan yang lainnya. Untuk pengguna Linux Debian atau Ubuntu, bisa langsung menginstall dengan command berikut ini:

```
$sudo apt install php-json php-mysqlnd php-xml php-intl
```

Untuk pengguna OS X bisa menginstall melalui Home Brew. Jika PHPmu versi 7.2 silahkan ketik command di bawah ini pada terminal:

```
brew install php@7.2-intl
```

Untuk menggunakan CI4, instalasi dapat dilakukan dengan 2 (dua) cara, yaitu:

- Download Codeigniter 4 di situs resminya
    - Visit >> https://codeigniter.com/en/download
  - Setelah download, pindahkan file ke folder htdocs (di asumsikan menggunakan XAMPP).
    - Extract .zip hasil download.
    - Rename folder menjadi ci404jwt (sebagai folder project).

- Install melalui composer
    - Buka CMD / terminal, emudian ketik command berikut:

  composer create-project codeigniter4/appstarter project-root
  // then
  cd project-root
  // then
  composer update

Ada 2 (dua) opsi untuk menjalankan aplikasi.

- Pertama, Jalankan xampp dan buka browser dan kemudian ketik: http://localhost/ci404jwt/public
- Kedua, tanpa harus menjalankan xampp, melalui terminal:
    - Dari terminal c:/xampp/htdocs/ci404jwt jalankan:

  php spark serve
    - Kemudian langsung buka browser dan akses via url: http:/localhost:8080

c. Membuat koneksi ke database

- Pertama, membuat database baru dengan nama ci4_auth_jwt.
- Kedua, Rename file **env** di folder project menjadi **.env** (tambahkan titiknya).
- Ketiga, dari kode berikut ini:

CI_ENVIRONMENT = production

Ubah menjadi:

CI_ENVIRONMENT = development

- Keempat, atur konfigurasi database dengan cara memodifikasi file .env menjadi:

  database.default.hostname = localhost

  database.default.database = ci4_auth_jwt

  database.default.username = root

  database.default.password =

  database.default.DBDriver = MySQLi

  Pada kode tersebut, memberikan nama database, username dan password sesuai rancangan yang di buat.

d. Membuat table

Salah satu cara membuat table di database menggunakan CI4 adalah:

- Dari folder project, perintah di bawah ini untuk membuat file migrasi:

  php spark migrate:create users

- dilanjutkan memodifikasi file users.php sebagai file migrasinya pada direktori app/Database/Migrations/~~tgl-date-time~~_users.php.

  Silahkan isi dengan kode berikut ini:

```
<?php namespace App\Database\Migrations;
use CodeIgniter\Database\Migration;
class Users extends Migration {
  public function up() {
    $this->forge->addField([
      'id' => [
        'type' => 'INT',
        'constraint' => 11,
        'auto_increment' => TRUE
      ],
      'first_name' => [
```

```
            'type' => 'VARCHAR',
            'constraint' => 100
          ],
          'last_name' => [
            'type' => 'VARCHAR',
            'constraint' => 100
          ],
          'email' => [
            'type' => 'VARCHAR',
            'constraint' => 100
          ],
          'password' => [
            'type' => 'VARCHAR',
            'constraint' => 100
          ]
        ]);
        $this->forge->addKey('id');
        $this->forge->createTable('users');
      }
      public function down() {
      }
  }
```

- Selesai edit dilanjutkan untuk migrate script table yang dibuat diatas agar tereksekusi ke database, silahkan ketik perintah berikut ini:

  php spark migrate

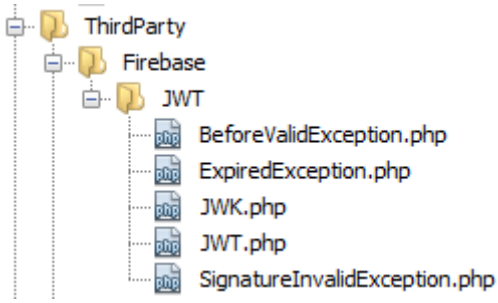
- Jika berhasil, di database akan memiiki table users.

e. Download atau Clone Package Firebase/JWT

- Bagian ini adalah pemanfaatan JWT (JSON Web Token) untuk pengembangan APInya dan dapat di download di link url https://github.com/firebase/php-jwt.
- Atau dengan cara clone dari folder project dengan masuk ke path ThirdParty dengan cara cd ThirdParty, dan eksekusi perintah berikut ini:

```
git clone https://github.com/firebase/php-jwt.git
```

- kemudian jadikan file hasil download ataupun hasil clone menjadi didalam folder project berikut ini:



- Lanjutkan dengan buka file Autoload.php pada folder project app/Config/Autoload.php dan edit isinya tambahkan seperti berikut:

```
public $psr4 = [
    APP_NAMESPACE => APPPATH, // For custom app namespace
    'Config' => APPPATH . 'Config',
    'Firebase' => APPPATH . 'ThirdParty/Firebase',
];
```

menambahkan seperti di anak panah diatas untuk memberikan inisialisasi name **Firebase** agar menuju ke **ThirdParty/Firebase**.

f. Membuat Model

- Membuat class dalam file Auth_model.php untuk menangani proses register dan cek login berdasarkan email.

```
<?php
 namespace App\Models;
 use CodeIgniter\Model;
 class Auth_model extends Model{
   protected $table = "users";
   public function register($data)  {
    $query=$this->db->table($this->table)-
>insert($data);
    return $query ? true : false;
  }
   public function cek_login($email)  {
    $query = $this->table($this->table)
        ->where('email', $email)
        ->countAll();
```

```
        if($query > 0){
          $hasil = $this->table($this->table)
              ->where('email', $email)
              ->limit(1)
              ->get()
              ->getRowArray();
        } else {
          $hasil = array();
        }
        return $hasil;
    }
}
```

- Simpan di folder project app/Models.

g. Membuat file Controller

Membuat 2 (dua) controller yang berbeda. **Pertama** membuat controller **Auth.php** yang bertugas menangani login, register, dan generate token. **Kedua**, mengubah controller **Home.php** sebagai halaman final yang bisa diakses jika user telah memasukan header (bearer Token) ke dalam request.

Berikut kode untuk Auth.php:

```
<?php namespace App\Controllers;
use \Firebase\JWT\JWT;
use App\Models\Auth_model;
use CodeIgniter\RESTful\ResourceController;
class Auth extends ResourceController {
  public function __construct()  {
    $this->auth = new Auth_model();
  }
  public function privateKey()  {
    $privateKey = "<<<EOD
      -----BEGIN RSA PRIVATE KEY-----
eUz9sHyD6vkgZzjtxXECQAkp4Xerf5TGfQXGXhxIX52yH+N2
LtujCdkQZjXAsGd
      -----END RSA PRIVATE KEY-----
      EOD";
    return $privateKey;
  }
  public function register() {
```

```
    $firstname          =          $this->request-
>getPost('first_name');
    $lastname              =       $this->request-
>getPost('last_name');
    $email   = $this->request->getPost('email');
    $password              =       $this->request-
>getPost('password');
    $password_hash=password_hash($password,
PASSWORD_BCRYPT);

    $data                                          =
json_decode(file_get_contents("php://input"));

    $dataRegister = [
      'first_name' => $firstname,
      'last_name' => $lastname,
      'email' => $email,
      'password' => $password_hash
    ];
    $register           =           $this->auth-
>register($dataRegister);
    if($register == true) {
      $output = [
        'status' => 200,
        'message' => 'Berhasil register'
      ];
      return $this->respond($output, 200);
    } else {
      $output = [
        'status' => 400,
        'message' => 'Gagal register'
      ];
      return $this->respond($output, 400);
    }
  }

  public function login() {
    $email   = $this->request->getPost('email');
    $password              =       $this->request-
>getPost('password');
```

```
    $cek_login = $this->auth->cek_login($email);


if(password_verify($password,$cek_login['passwor
d'])){
      $secret_key = $this->privateKey();
      $issuer_claim = "THE_CLAIM";
      $audience_claim = "THE_AUDIENCE";
      $issuedat_claim = time(); // issued at
      $notbefore_claim = $issuedat_claim + 10;
      $expire_claim = $issuedat_claim + 3600;
      $token = array(
        "iss" => $issuer_claim,
        "aud" => $audience_claim,
        "iat" => $issuedat_claim,
        "nbf" => $notbefore_claim,
        "exp" => $expire_claim,
        "data" => array(
          "id" => $cek_login['id'],
          "firstname"                          =>
$cek_login['first_name'],
          "lastname" => $cek_login['last_name'],
          "email" => $cek_login['email']
        )
      );

      $token = JWT::encode($token, $secret_key);

      $output = [
        'status' => 200,
        'message' => 'Berhasil login',
        "token" => $token,
        "email" => $email,
        "expireAt" => $expire_claim
      ];
      return $this->respond($output, 200);
    } else {
      $output = [
        'status' => 401,
        'message' => 'Login failed',
        "password" => $password
      ];
      return $this->respond($output, 401);
```

```
    }
  }
}
```

Kemudian pada Home.php, diubah menjadi ini kodenya:

```
<?php namespace App\Controllers;
use \Firebase\JWT\JWT;
use App\Controllers\Auth;
use CodeIgniter\RESTful\ResourceController;

header("Access-Control-Allow-Origin: * ");
header("Content-Type:           application/json;
charset=UTF-8");
header("Access-Control-Allow-Methods: POST");
header("Access-Control-Max-Age: 3600");
header("Access-Control-Allow-Headers:    Content-
Type,               Access-Control-Allow-Headers,
Authorization, X-Requested-With");

class Home extends ResourceController {
  public function __construct() {
    $this->protect = new Auth();
  }

  public function index() {
    $secret_key = $this->protect->privateKey();
    $token = null;
    $authHeader=$this->request-
>getServer('HTTP_AUTHORIZATION');
    $arr = explode(" ", $authHeader);
    $token = $arr[1];

     if($token){

       try {

     $decoded=JWT::decode($token,$secret_key,
array('HS256'));

        if($decoded){
          $output = [
            'message' => 'Access granted'
          ];
```

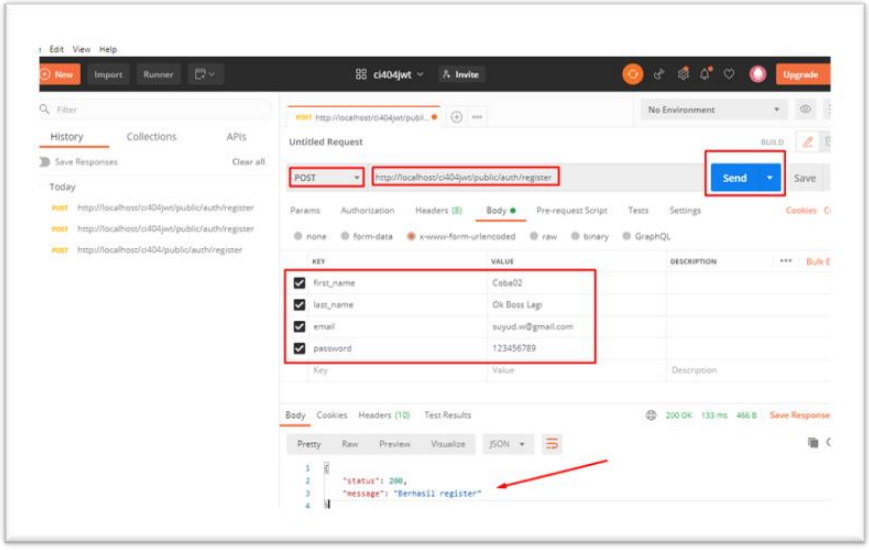
```
                return $this->respond($output, 200);
            }

        } catch (\Exception $e){

            $output = [
                'message' => 'Access denied',
                "error" => $e->getMessage()
            ];

            return $this->respond($output, 401);
        }
    }
}
```

h. Compiling dan Testing



Daftar Referensi

Goggin, Gerrard. (2006). *Cell Phone Culture: Mobile Technology in Everyday Life*. USA: Routledge.

Griffin, EM. (2000). *A first Look At Communication Theory. Fourth edition.* McGraw: Hill Companies. 2000.

Horst, Heather A. dan Daniel Miller. (2006). *The Cell Phone: And Anthropology of Communication*. UK: Biddles Ltd. 2006.

Ling, Rich, Jonathan Donner. (2006). *Mobile Communication: Digital Media and Series*. UK: Polity Press. 2009.

Rogers, Everette M. (1986). *Communication Technology: The New Media in Society*. London: Collier Macmillan Publisher, 1986

Rajamani Ganesh, Kaveh Pahlawan, Zoran Zvonar. (2004). *WIRELESS MULTIMEDIA NETWORK TECHNOLOGIES*, Kluwer Academic Publishers, London, Moscow.

Gail Rahn Frederick, Rajesh Lal. (2009). *Beginning Smartphone Web Development: Building JavaScript, CSS, HTML and Ajax-based Applications for iPhone, Android, Palm Pre, BlackBerry, Windows Mobile, and Nokia S60*. Springer-Verlag New York, 2009

Anugrah Sandi. (2017, 16 November) *Mengenal Apa itu Web API* Diakses pada 01 November 2020, dari https://www.codepolitan.com/mengenal-apa-itu-web-api-5a0c2855799c8

codeigniter4.github.io. (2019) *RESTful Resource Handling* Diakses pada 01 November 2020, dari https://codeigniter4.github.io/userguide/incoming/restful.html

idntimes.com. (2020, 02 Januari) *Prediksi 7 Tren Teknologi Mutakhir yang akan Berkembang di Tahun 2020* Diakses pada 20 Oktober 2020, dari https://www.idntimes.com/tech/trend/izza-namira-1/prediksi-7-tren-teknologi-mutakhir-yang-akan-berkembang-di-tahun/7

ilmucoding.com (2020, 4 April) *Tutorial Cara Membuat CRUD REST API Codeigniter 4* Diakses pada 20 Oktober 2020, dari https://ilmucoding.com/rest-api-codeigniter-4/

M Fikri Setiadi. (2020, 05 July) *Tutorial Membuat RESTful API dengan CodeIgniter 4 (Panduan Lengkap).* Diakses pada 01 November 2020, dari http://mfikri.com/artikel/restful-api-codeigniter4

qwords.com. (2020, 22 August). *Mengenal Teknologi Smart Home System dan Cara Kerjanya*. Diakses pada 20 Oktober 2020, dari https://qwords.com/blog/teknologi-smart-home/

Rafki Fachrizal. (2019, 20 April) *Manfaat AI di Kamera Smartphone*. Diakses pada 20 Oktober 2020, dari https://infokomputer.grid.id/read/121702692/apa-sih-manfaat-ai-di-kamera-smartphone-begini-penjelasannya

Subari. (2008, 01 Maret). *Smart Home, sistem pintar di rumah*. Diakses pada 13 Oktober 2020, dari https://subaridargombez.wordpress.com/2008/03/01/smart-home-sistem-pintar-di-rumah-2/

sis.binus.ac.id. (2018, 09 Maret) *PERKEMBANGAN TEKNOLOGI 1G, 2G, 3G, 3.5G, 4G DAN 5G* Diakses pada 20 Oktober 2020, dari https://sis.binus.ac.id/2018/03/09/perkembangan-teknologi-1g-2g-3g-3-5g-4g-dan-5g/

DIPLOMASI SIBER DAN TEKNOLOGI MOBILE PADA MULTIDISIPLIN

MUHAMMAD RIDHA ISWARDHANA, S.I.P., M.A.
SUYUD WIDIONO, S.PD., M.KOM.

Buku ini terbagi tersusun dari dua latar belakang keilmuan, yang pertama membahas tentang diplomasi siber dan upaya perlindungan terhadap Ancaman penggunaan teknologi informasi di Indonesia, dan yang kedua membahas tentang teknologi mobile. Harapannya buku ini dapat menjadi referensi kepada masyarakat luas tentang teknologi yang sedang marak belakangan ini.

P.A.C.E

Partnership for Action on Community Education
Jl. Subarang Koto Baru, Kubung, Solok-Sumatera Barat
Komplek Pondok Pinang, Padang-Sumatera Barat

TAHUN 2021

ISBN 978-623-97711-0-2

9 786239 771102