Society

Society, 8 (2), 662-673, 2020
P-ISSN: 2338-6932 | E-ISSN: 2597-4874
https://society.fisip.ubb.ac.id

Penerapan Tanda Tangan Digital sebagai Bentuk Baru Penyelenggaraan *Smart Governance*

Nursani Budiarti [1,*] Yahya Pandega Putra [1,] dan Achmad Nurmandi [2]
[1] Magister Ilmu Pemerintahan, Jusuf Kalla School of Government,
Universitas Muhammadiyah Yogyakarta, 55183, Yogyakarta, Indonesia
[2] Program Studi Politik Islam - Ilmu Politik, Jusuf Kalla School of Government,
Universitas Muhammadiyah Yogyakarta, 55183, Yogyakarta, Indonesia
* Korespondensi: nursani.budiarti@gmail.com

INFO ARTIKEL

Info Publikasi:
Studi Pustaka

Sitasi Cantuman:
Budiarti, N., Putra, Y. P., & Nurmandi, A. (2020). Digital Signature Implementation as a New Smart Governance Model. Society, 8(2), 628-639.

DOI: *10.33019/society.v8i2.222*

Dikirim: 22 Agustus, 2020;
Diterima: 9 November, 2020;
Dipublikasi: 30 Desember, 2020;

ABSTRAK

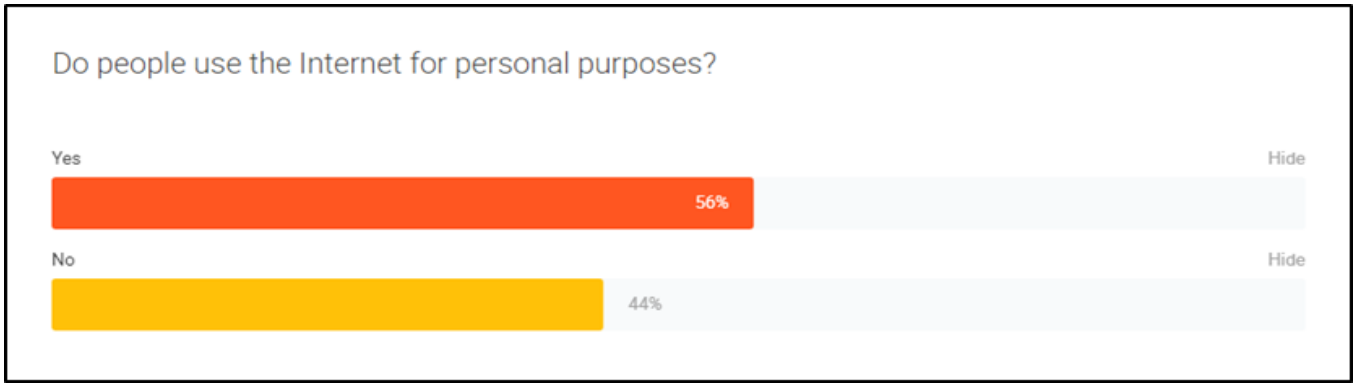
Dengan perkembangan zaman, tidak ada yang mustahil dengan teknologi internet. Salah satu kelebihan dari internet adalah memungkinkan untuk dikembangkan untuk mendukung kreativitas dan keterbukaan kepada publik, khususnya tata kelola pemerintahan berbasis Teknologi Informasi dan Komunikasi (TIK) atau smart governance, dengan penerapan tanda tangan digital, baik dalam penyelenggaraan pelayanan publik maupun dalam korespondensi dan dokumen lainnya. Sebagian besar studi tanda tangan digital sebelumnya terbatas pada penelitian teknis tentang pola dan desain tanda tangan digital. Penelitian ini bertujuan untuk mendeskripsikan penerapan tanda tangan digital sebagai bentuk baru penyelenggaraan smart governance. Penelitian ini menggunakan metode penelitian kualitatif dan sumber data yang terdiri dari data referensi dari berbagai penelitian sebelumnya dan data bersumber dari berita media online nasional. Berdasarkan hasil analisis menggunakan perangkat lunak NVivo 12 Plus, diperlukan penerapan tanda tangan digital (digital signature) untuk mengantisipasi ancaman kejahatan dunia maya (cybercrime) dalam penyelenggaraan pelayanan publik yang efektif, efisien, dan akuntabel sebagai bentuk baru penyelenggaraan smart governance.

Kata Kunci: *Keamanan Siber; Kejahatan Dunia Maya; Pelayanan Publik; Smart Governance; Tanda Tangan Digital*

1. Pendahuluan

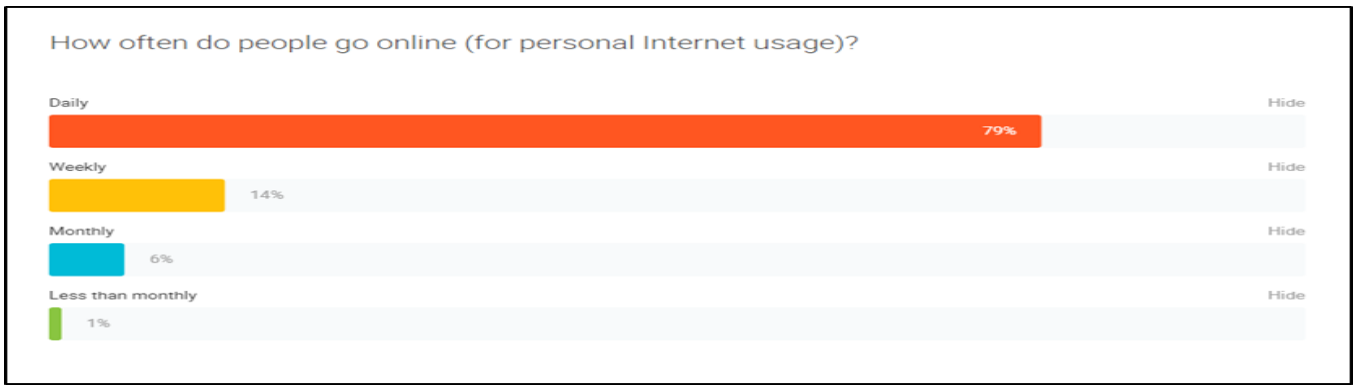
Semakin pesat perkembangan teknologi maka akan semakin banyak pula tantangan yang muncul bersamanya. Dengan kemajuan teknologi, setiap orang dapat dengan mudah melakukan segala sesuatu dengan lebih cepat dan lebih singkat. Salah satu perkembangan teknologi tersebut adalah internet. Mayoritas pengguna internet di Indonesia menggunakan internet dalam kehidupan sehari-hari (Darmayani, 2018). Saat ini internet tidak hanya digunakan sebagai penunjang pekerjaan, tetapi internet juga telah menjadi bagian yang tidak terpisahkan dari kehidupan manusia. Karenanya, pengaruh internet ada di setiap aspek kehidupan manusia. Selain digunakan sebagai penunjang kerja, juga untuk kebutuhan pribadi setiap orang. Internet telah menjadi pintu dan jendela dunia, dunia yang lebih luas dan tanpa batas. Tidak ada yang mustahil dengan teknologi internet, mulai dari hal yang paling sederhana yaitu mencari berita hingga berkomunikasi dengan kerabat atau teman di belahan dunia lain. Salah satu kelebihan dari internet adalah memungkinkan untuk dikembangkan guna menunjang kreativitas dan keterbukaan kepada publik. Hal tersebut menjadikan internet sangat fleksibel untuk perkembangan selanjutnya yang mendorong muncul dan berkembangnya inovasi *online* (Septianingrum *et al.*, 2018).

Terkait penggunaan internet saat ini, data yang dilaporkan oleh Google Consumer Barometer berdasarkan hasil survei tahun 2017 menunjukkan bahwa sebagai berikut:



Gambar 1. Penggunaan Internet untuk Keperluan Pribadi
Sumber: Google Consumer Barometer (2017a)

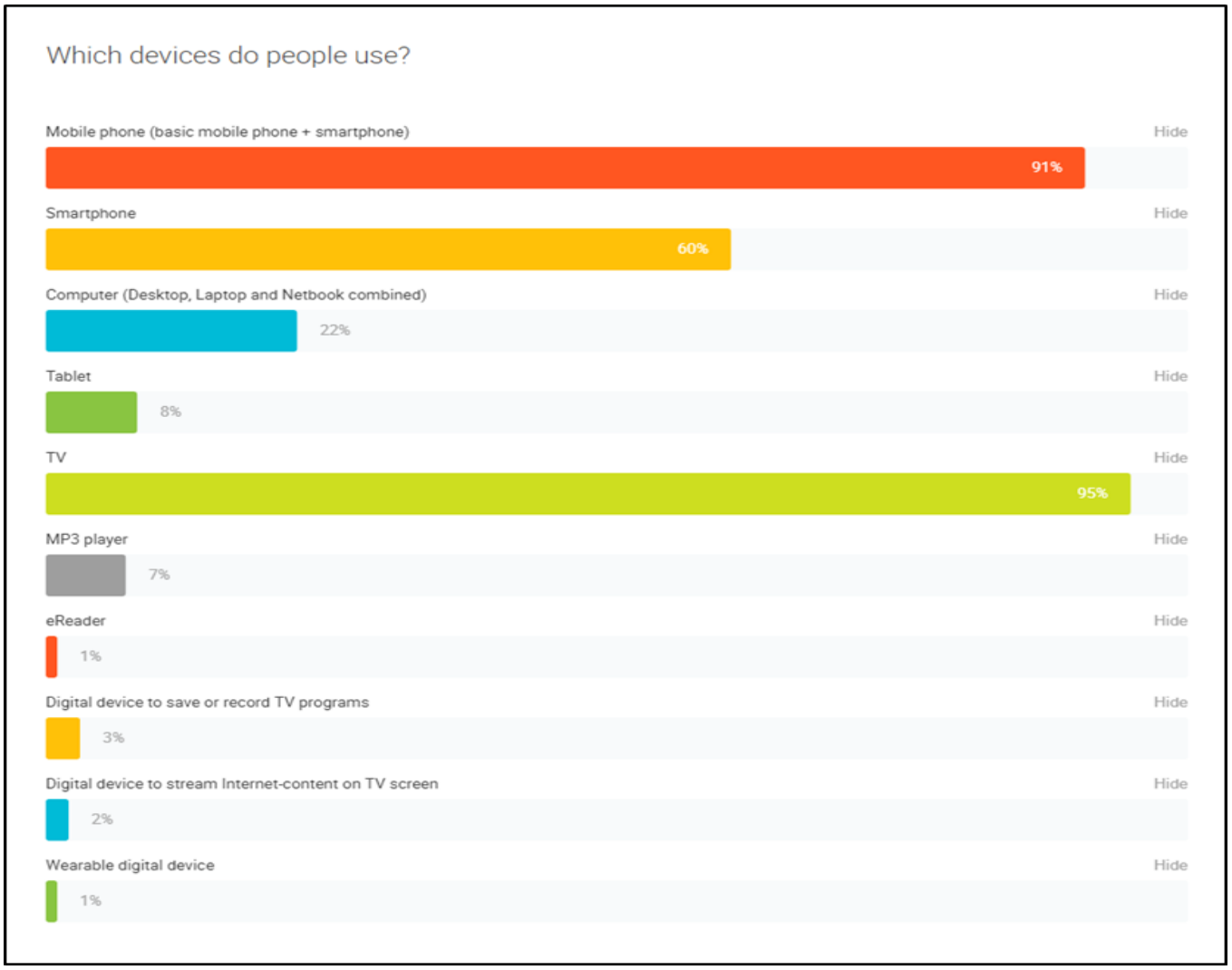
Berdasarkan **Gambar 1**, dari populasi 1.000 responden *online* dan *offline* tahun 2017, 56% responden menggunakan internet untuk keperluan pribadi, dan 44% menggunakan internet, bukan untuk keperluan pribadi.



Gambar 2. Penggunaan Internet Pribadi
Sumber: Google Consumer Barometer (2017b)

https://doi.org/10.33019/society.v8i2.222

Berdasarkan **Gambar 2**, dari populasi 604 responden *online* pada tahun 2017 yang mengakses melalui komputer, *Tablet*, dan *Smartphone* untuk keperluan pribadi, terlihat bahwa 79% responden mengakses internet setiap hari, 14% mengakses internet seminggu sekali, 6% mengakses internet sebulan sekali, dan 1% responden mengakses internet kurang dari sebulan sekali.



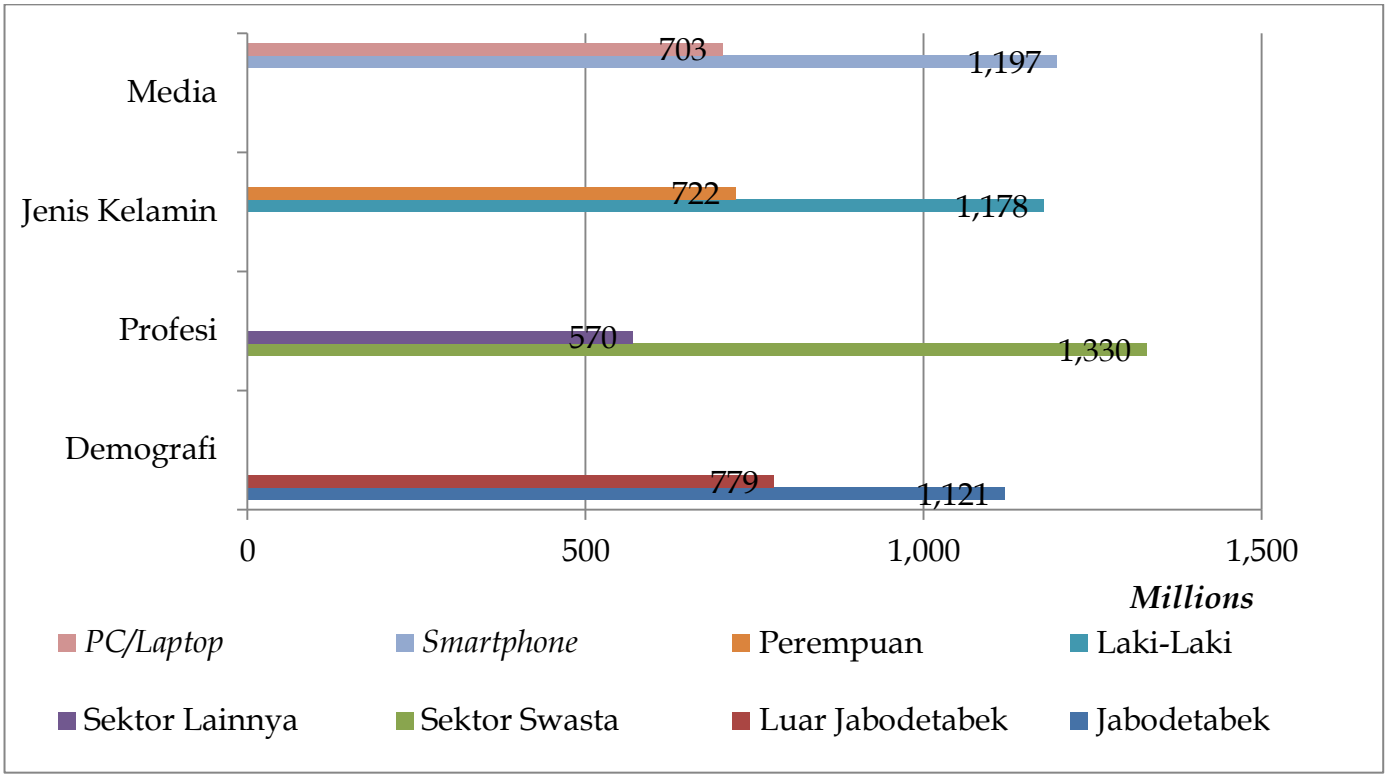
Gambar 3. Perangkat yang digunakan
Sumber: Google Consumer Barometer (2017c)

Berdasarkan **Gambar 3**, dari populasi 1.000 responden *online* dan *offline* pada tahun 2017, 91% mengakses internet melalui telepon seluler (telepon seluler dan *Smartphone*). Selain itu, 60% menggunakan *Smartphone*, 22% menggunakan komputer (gabungan Desktop, Laptop, dan Notebook), 8% menggunakan *Tablet*, 95% menggunakan televisi, 7% menggunakan *MP3 player*, 1% menggunakan *eReader*, 3% menggunakan perangkat digital untuk menyimpan atau merekam program TV, 2% perangkat digital untuk melakukan *streaming* konten internet di layar TV dan 1% menggunakan perangkat digital *wearable*.

Ketiga gambar di atas menunjukkan bagaimana pola perkembangan teknologi khususnya internet yang semakin masif. Hal tersebut memaksa pemerintah untuk menyiapkan standar keamanan siber (*cybersecurity*). Tanpa standar keamanan siber (*cybersecurity*) yang aman dan tepat, ancaman akan terus meningkat. Salah satu langkah keamanan siber pemerintah adalah

https://doi.org/10.33019/society.v8i2.222

dengan menerapkan tanda tangan digital (*digital signature*) pada dokumen resmi pemerintah. Tanda tangan digital terdiri dari informasi elektronik yang berkaitan dengan informasi elektronik lainnya sebagai sistem verifikasi atau otentikasi. Di Indonesia, perusahaan digital yang memiliki kewenangan untuk menerima pendaftaran, verifikasi, dan penerbitan sertifikat elektronik dan tanda tangan elektronik bagi warga negara Indonesia serta telah terdaftar dan diakui oleh Kementerian Komunikasi dan Informatika Republik Indonesia dengan nama PrivyID.



Gambar 4. Pengguna Tanda Tangan Digital PrivyID Tahun 2018
Sumber: Selular.id (2018)

Berdasarkan **Gambar 4**, pada 2018, pengguna tanda tangan digital PrivyID adalah 1,9 juta. Berdasarkan demografi, 59% pengguna tanda tangan digital berada di Jakarta-Bogor-Depok-Tangerang-Bekasi (Jabodetabek) dan 41% di luar Jabodetabek. Jika dipilah berdasarkan profesi, 70% pengguna tanda tangan digital pada 2018 adalah pekerja swasta, dan 30% adalah pekerja sektor lainnya. Sedangkan jika dipilah berdasarkan jenis kelamin, 62% adalah pengguna laki-laki, dan 38% adalah pengguna perempuan. Berdasarkan penggunaan media operasi, sebanyak 63% pengguna menandatangani dokumen melalui *smartphone*, dan sekitar 37% menggunakan komputer pribadi (PC) atau laptop.

2. Tinjauan Pustaka

Perkembangan TIK, yang terdiri dari *Internet of Things* (*IoT*), *Internet of Everything (IoE)*, dan *Internet of Nano Things (IoNT)*, merupakan pendekatan baru untuk mengintegrasikan internet ke dalam kehidupan personal, profesional, dan masyarakat (Miraz *et. al.*, 2015). Banyak kota atau daerah menggunakan pendekatan ini untuk menyelenggarakan pemerintahan, perencanaan, dan pengelolaan kota atau wilayah.

Secara umum, untuk disebut kota atau daerah yang besar dan sejahtera, kota-kota di seluruh dunia memiliki kualitas dan standar yang baik dalam berbagai aktivitas dan kehidupan

https://doi.org/10.33019/society.v8i2.222

masyarakat. Perencanaan kota dan daerah diperlukan untuk meningkatkan tata kelola pemerintahan, inovasi teknologi, kesejahteraan masyarakat, dan kualitas investasi bisnis untuk mewujudkan *Smart City*. Predikat *Smart City* diperoleh dengan mengembangkan tata kelola infrastruktur cerdas (*Smart Infrastructure*) menggunakan Teknologi Informasi dan Komunikasi (TIK) untuk mencari dan menganalisis data yang dibutuhkan oleh pemerintah, masyarakat, dan pemangku kepentingan (*Stakeholders*) lainnya. Menjadi *Smart City* juga berarti harus terus berinovasi dan berkembang ke arah yang lebih baik.

Smart governance menjadi syarat utama dalam melaksanakan pembangunan *Smart City*. Pemerintah harus membentuk paradigma masyarakat tentang kehidupan yang lebih baik. Kepercayaan publik terhadap pemerintah dapat ditumbuhkan dengan menunjukkan kepedulian dan transparansi dalam penyelenggaraan pemerintahan. Dalam melaksanakan tata kelola pemerintahan, konsep tata kelola yang baik (*good governance*) merupakan kunci utama keberhasilannya. Konsep tersebut merupakan paradigma, sistem dan tata kelola pemerintahan serta pembangunan yang berdasarkan prinsip hukum. *Smart governance* bertujuan untuk mewujudkan tata kelola yang efektif, efisien, komunikatif, serta terus meningkatkan kinerja birokrasi melalui inovasi dan adopsi teknologi yang terintegrasi.

Pola perkembangan teknologi yang semakin masif, khususnya internet, memaksa pemerintah untuk mempersiapkan standar keamanan siber untuk jaringan internet yang ada, khususnya penyelenggaraan pemerintahan berbasis TIK. Tanpa standar *cybersecurity* yang cepat dan tepat, ancaman akan semakin meningkat yang disebut *cybercrime* (kejahatan dunia maya). *Cybercrime* adalah aktivitas melanggar hukum di mana komputer atau perangkat komputasi seperti *smartphone*, *tablet*, *Personal Digital Assistant* (PDA), dan perangkat lain yang berdiri sendiri atau bagian dari jaringan (*network*) digunakan sebagai alat dan atau sebagai sasaran untuk aktivitas kriminal. Orang-orang dengan pola pikir destruktif dan kriminal sering melakukan kejahatan dunia maya (*cybercrime*) untuk membalas dendam, keserakahan, dan mendapatkan pengalaman (Pande, 2017).

Jenis ancaman *cybercrime* terdiri dari 1) Pencurian data pribadi untuk tujuan komersial, seperti pencurian identitas dan nomor kartu kredit; 2) Akses ilegal ke data perusahaan yang digunakan untuk persaingan bisnis; 3) Pencurian data pemerintah yang digunakan untuk menyerang entitas tertentu; 4) Mengumpulkan data intelijen suatu negara untuk kepentingan negara asing atau entitas tertentu; 5) Manipulasi data untuk tujuan politik atau bisnis; 6) Serangan yang bertujuan menghilangkan kendali atau melemahkan atau bahkan melumpuhkan pemerintah atau perusahaan; 7) Manipulasi perilaku pengguna internet untuk mengunduh *Malicious Software (Malware)* yang bertujuan untuk menyusup dan menghancurkan sistem, dan 8) Serangan langsung melalui jaringan internet terhadap sistem yang bertujuan untuk melumpuhkan layanan publik dari lembaga publik tertentu (Ahmad *et al.*, 2018) .

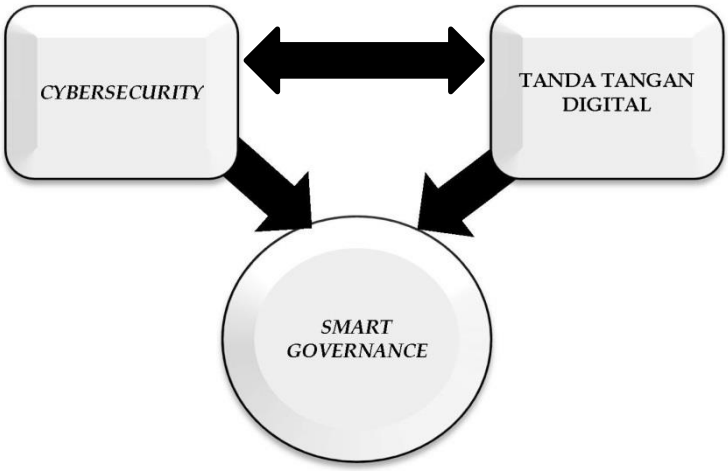
Proses tata kelola berbasis TIK memangkas birokrasi yang panjang menjadi proses pelayanan publik yang efektif dan efisien tanpa bertentangan dengan peraturan perundang-undangan yang berlaku. Birokrasi terkadang menyebabkan keterlambatan dalam proses pelayanan publik dan pengambilan keputusan kebijakan pemerintah. Dalam melakukan penyederhanaan birokrasi diperlukan suatu sistem yang efektif dan efisien tanpa mengurangi akuntabilitas pemerintahan dengan penerapan tanda tangan digital pada pelayanan publik dan proses korespondensi serta dokumen administrasi pemerintahan lainnya. Tanda tangan digital terdiri dari informasi elektronik yang berkaitan dengan informasi elektronik lainnya sebagai sistem verifikasi atau otentikasi. Tanda tangan digital bukanlah tanda tangan yang dipindai dan kemudian disematkan ke dalam dokumen, melainkan serangkaian data dan informasi yang disematkan ke dalam dokumen.

https://doi.org/10.33019/society.v8i2.222

Tanda tangan digital merupakan salah satu kebijakan keamanan siber yang diterapkan dalam mengantisipasi manipulasi data dan dokumen resmi yang dikeluarkan. Tiga proses dasar tanda tangan digital terdiri dari pemeriksaan otentikasi penanda tangan, otentikasi dokumen, dan verifikasi tanda tangan digital. Pengembangannya menggunakan beberapa algoritma, seperti Elgamal dan Schnorr (Pooja & Yadav, 2018).

Penerapan tanda tangan digital dalam pemerintahan semakin meningkat, mulai dari pengelolaan dokumen dalam korespondensi resmi hingga digunakan dalam dokumen perizinan pemerintah. Penggunaan tanda tangan digital dapat menjamin bahwa dokumen tersebut asli (Liyanti & Hakim, 2019) karena dapat mengotentikasi dokumen yang ditandatangani dan pemilik tanda tangan melalui suatu algoritma (Perdana *et al.*, 2019). Ada dua jenis tanda tangan digital: tanda tangan digital tidak bersertifikasi (*uncertified digital signature)* dan tanda tangan digital bersertifikasi (*certified digital signature*). Jenis tanda tangan digital yang tidak bersertifikasi misalnya adalah tanda tangan tinta basah yang dipindai, *Barcode*, *QR Code*, dan Biometrik. Sebaliknya, contoh tanda tangan digital bersertifikasi adalah tanda tangan yang menggunakan kriptografi atau disebut tanda tangan digital (*digital signature*).

Tanda tangan digital sebagai bentuk baru penyelenggaraan *smart governance* bertujuan untuk mendorong *smart governance* yang akuntabel lebih lanjut untuk mengembangkan keamanan siber (cybersecurity) (Febrianta *et al.*, 2019). Selain itu, penerapan kebijakan tanda tangan digital (*digital signature*) juga sejalan dengan penerapan *smart governance* terutama dalam tata kelola pemerintahan yang baik, serta terciptanya citra positif pemerintahan yang modern dan progresif (Kumar, 2015).



Gambar 5. Kerangka Konseptual

Gambar 5 di atas menggambarkan bahwa kerangka konseptual studi dari konsep *smart governance* menekankan pada kebijakan *cybersecurity* dengan penerapan tanda tangan digital untuk mengantisipasi manipulasi data dan dokumen resmi yang dikeluarkan pemerintah untuk melaksanakan proses tata kelola pemerintahan yang efektif, efisien, dan akuntabel.

3. Metodologi Penelitian

Kerangka konseptual studi ini berdasarkan penyelenggaraan *smart governance* membutuhkan kebijakan *cybersecurity* menggunakan tanda tangan digital (*digital signature*) (**Gambar 5**). Penelitian ini bertujuan untuk mendeskripsikan penerapan tanda tangan digital

https://doi.org/10.33019/society.v8i2.222

sebagai bentuk baru penyelenggaraan *smart governance* untuk mengimplementasikan pelayanan publik yang efektif, efisien, dan akuntabel.

Penelitian ini menggunakan metode penelitian kualitatif dan sumber data yang terdiri dari data referensi dari berbagai penelitian sebelumnya dan data yang bersumber dari berita media *online* nasional menggunakan perangkat lunak NVivo 12 Plus dengan fitur *NCapture*. Fitur ini mampu mengekstrak data secara sistematis dari media *online* nasional dengan menggali setiap berita secara mendalam. Penggunaan media *online* nasional dalam penelitian ini bertujuan untuk melengkapi *literature review* yang digunakan sebagai referensi. Penggunaan perangkat lunak NVivo 12 Plus bertujuan untuk memetakan dan mengeksplorasi implementasi kebijakan keamanan siber menggunakan tanda tangan digital dalam *smart governance*.

4. Hasil Penelitian dan Pembahasan

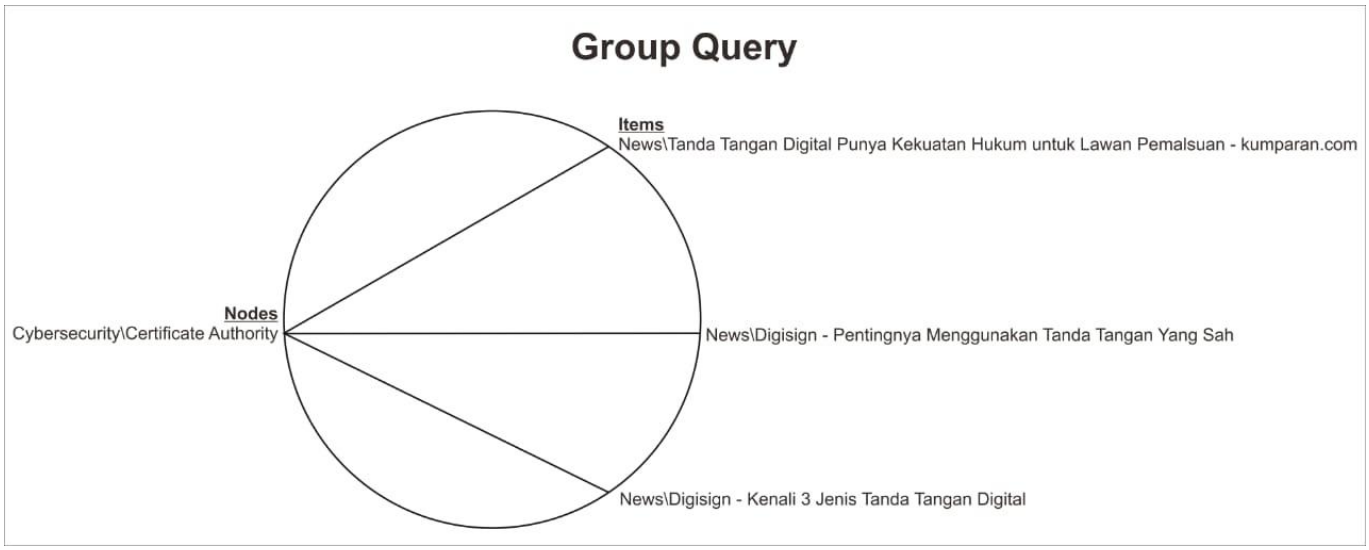
Beberapa fungsi dari implementasi *smart governance* adalah 1) Pembuatan kebijakan dan implementasi fungsi regulasi dan pembangunan berjalan dengan baik; 2) Akuisisi, penyimpanan, dan pengambilan data dilaksanakan dengan cepat; 3) Peningkatan manajemen tata kelola pemerintahan; 4) Peningkatan sosialisasi aturan, regulasi, dan kegiatan pemerintah; 5) Peningkatan kinerja dalam fungsi pengaturan; 6) Peningkatan kinerja di bidang sosial; dan 7) Menciptakan citra positif pemerintahan yang modern dan progresif (Kumar, 2015).

Gambar 6. *Smart Governance*
Sumber: NVivo 12 Plus (hasil data diolah)

Gambar 6 menunjukkan dua laporan media *online* nasional tentang *smart governance*, khususnya pemberitaan *smart city*, dan berita *online* nasional mengenai sertifikat elektronik. Sebagai bagian dari *smart city*, *smart governance* membutuhkan penerapan kebijakan pada sertifikat elektronik.

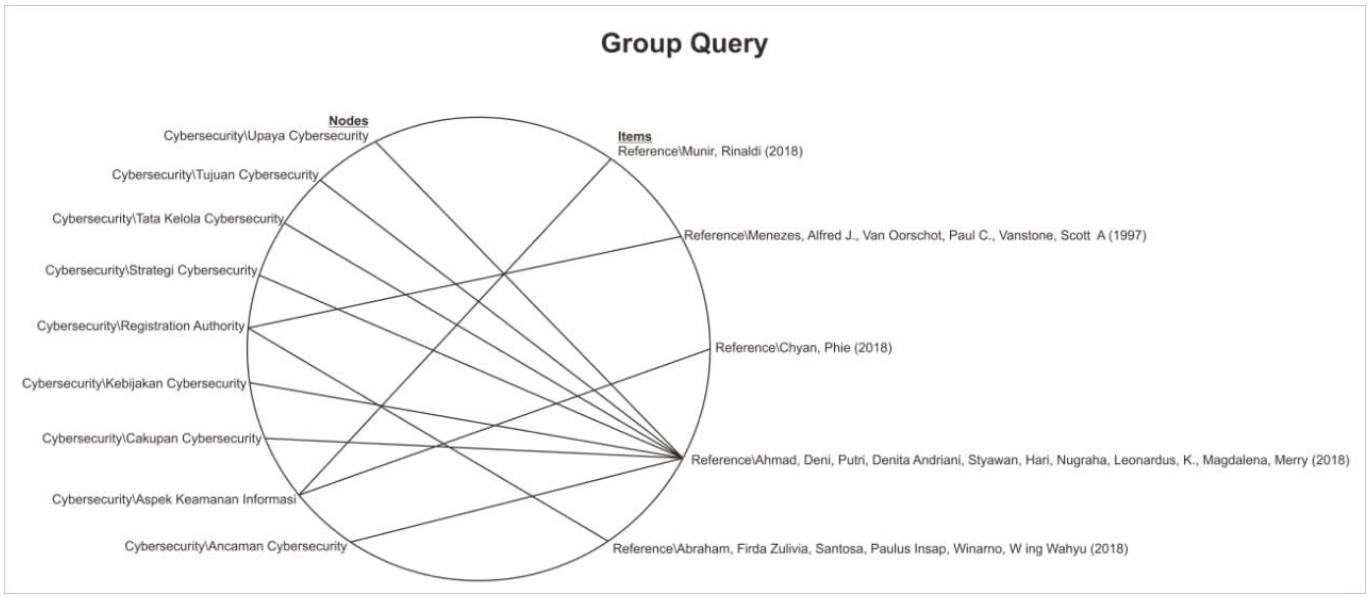
Pola perkembangan teknologi yang semakin masif, khususnya internet, memaksa pemerintah untuk mempersiapkan standar keamanan siber (*cybersecurity*) untuk jaringan internet yang ada, khususnya dalam penyelenggaraan pemerintahan berbasis TIK. Tanpa langkah-langkah keamanan siber yang cepat dan tepat, ancaman akan semakin meningkat yang disebut kejahatan siber (*cybercrime*).

https://doi.org/10.33019/society.v8i2.222



Gambar 7. *Cybersecurity*
Sumber: NVivo 12 Plus (hasil data diolah)

Gambar 7 menunjukkan bahwa beberapa berita *online* nasional melaporkan tentang kebijakan keamanan siber (*cybersecurity*). *Cybersecurity* merupakan kebijakan yang harus dilakukan pemerintah untuk mengantisipasi ancaman kejahatan dunia maya (*cybercrime*).



Gambar 8. Penelitian tentang *Cybersecurity*
Sumber: NVivo 12 Plus (hasil data diolah)

Gambar 8 menunjukkan bahwa ada lima penelitian yang mengkaji keamanan siber (*cybersecurity*), terdiri dari:

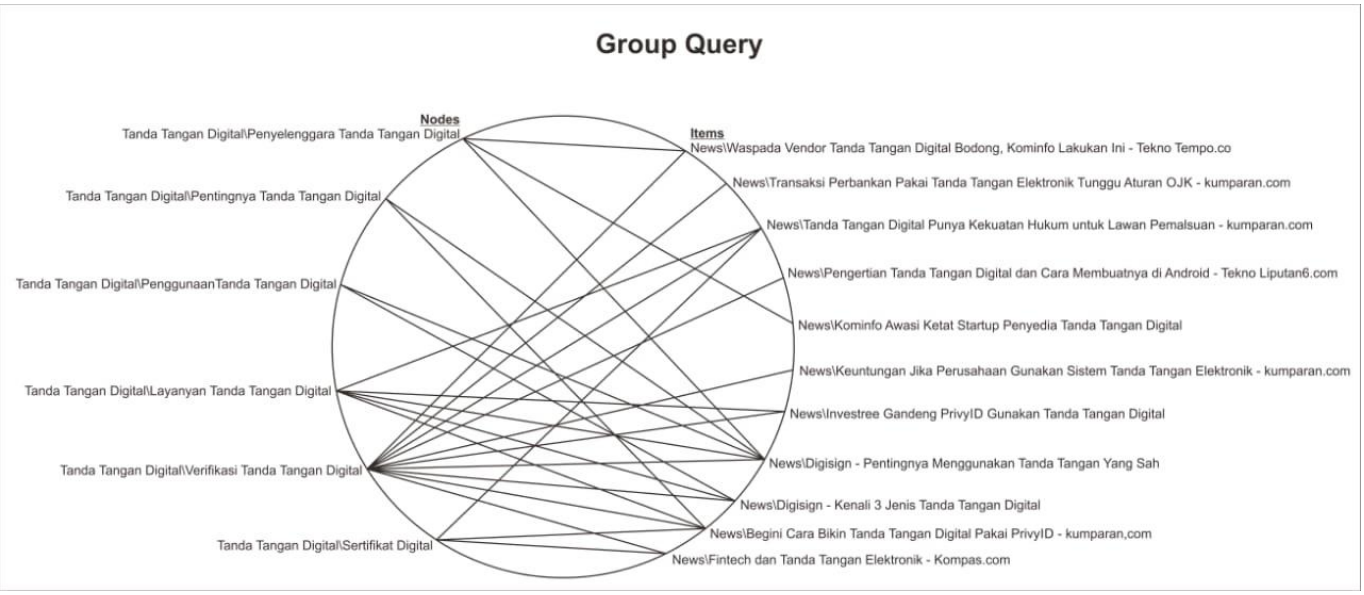
1) Rinaldi Munir melakukan kajian terhadap aspek keamanan informasi dan menyatakan bahwa tanda tangan digital (*digital signature*) tidak terbatas pada penyematan dokumen digital. Tanda tangan digital juga dapat disematkan dalam perangkat lunak (*software*) untuk menjaga integritas dokumen dan perangkat lunak (Munir, 2015).
2) Alfred J. Menezes, Paul C. van Oorschot, & Scott A. Vanstone, dalam buku yang berjudul "*Handbook of Applied Cryptography*" menjelaskan *registration authority*. Proses tersebut merupakan salah satu proses dalam penerbitan tanda tangan digital (*digital signature*) yang

https://doi.org/10.33019/society.v8i2.222

bertujuan untuk menjaga kerahasiaan, integritas, otentikasi entitas, dan otentikasi data (Menezes *et al.*, 1997).

3) Phie Chyan melakukan kajian terhadap aspek keamanan informasi dan menyatakan bahwa mengikuti keunggulan pengembangan TIK, ada satu hal yang harus menjadi perhatian pemerintah yaitu keamanan informasi. Informasi tersebut harus dijaga agar tidak diketahui oleh orang yang tidak berwenang (Chyan, 2018).
4) Deni Ahmad, Dinita Andriani Putri, Hari Styawan, Leonardus K. Nugraha, & Merry Magdalena melakukan kajian tentang kebijakan, tata kelola, strategi dan upaya, cakupan, sasaran, dan ancaman keamanan siber (*cybercrime*) (Ahmad *et al.*, 2018).
5) Firda Zulivia Abraham, Paulus Insap Santosa, & Wing Wahyu Winarno melakukan kajian *registration authority* yang merupakan model otentikasi tanda tangan digital yang digunakan untuk dokumen elektronik yang dibuat, dikirim, atau disimpan, baik dalam tipe analog atau digital atau dalam tipe lainnya (Abraham *et al.*, 2018).

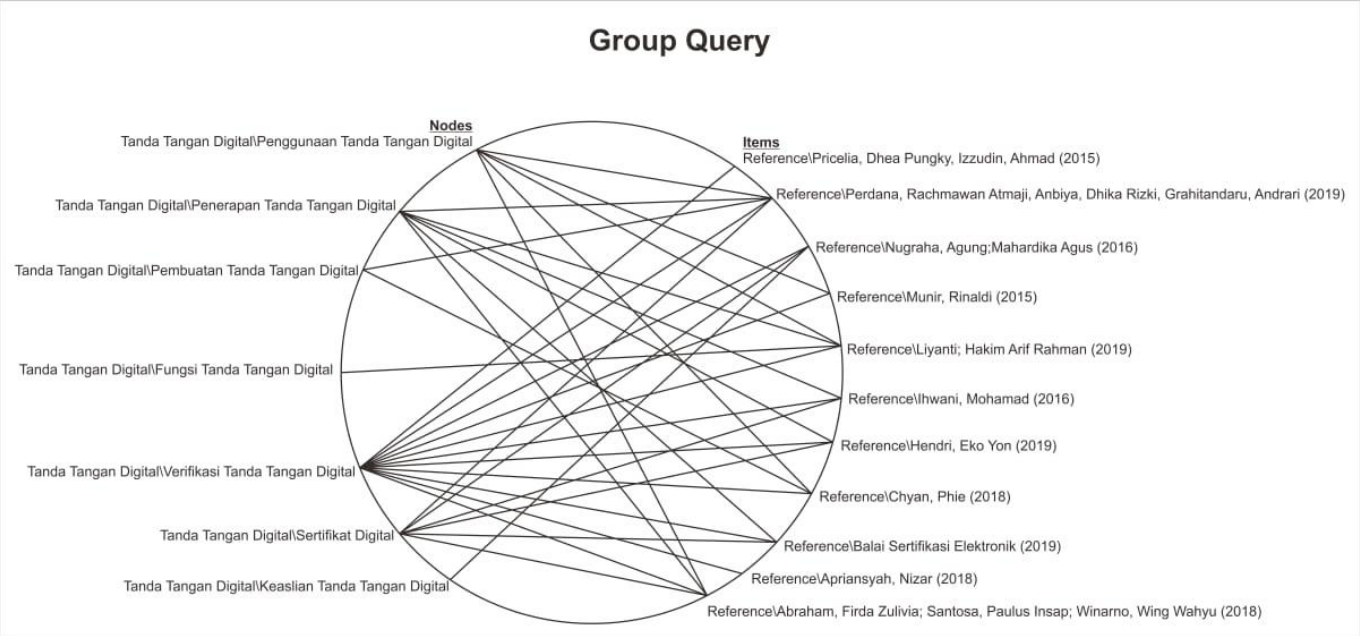
Pemerintah harus menerapkan kebijakan keamanan siber (*cybersecurity*) dalam proses tata kelola pemerintahan untuk mengantisipasi ancaman kejahatan dunia maya (*cybercrime)* dalam penyelenggaraan *smart governance*.



Gambar 9. ***Digital Signature***
Sumber: NVivo 12 Plus (hasil data diolah)

Gambar 9 menunjukkan bahwa banyak media *online* nasional memberitakan tentang penggunaan tanda tangan digital (*digital signature*). Proses validitas tanda tangan digital paling banyak diberitakan oleh sepuluh media *online* nasional. Sebagai perbandingan, layanan tanda tangan digital menempati urutan kedua dengan pemberitaan yang dilakukan oleh lima media *online* nasional, urutan ketiga mengenai validitas tanda tangan digital dengan menggunakan sertifikat digital dan penerapan tanda tangan digital yang diberitakan oleh tiga media *online* nasional dan selebihnya mengenai penggunaan dan pentingnya tanda tangan digital yang diberitakan oleh dua media *online* nasional. Tanda tangan digital dalam kerangka kebijakan keamanan siber (*cybersecurity)* dalam penerapan *smart governance* dinilai sebagai kebijakan yang tepat bagi banyak pihak.

https://doi.org/10.33019/society.v8i2.222



Gambar 10. Penelitian tentang *Digital Signature*
Sumber: NVivo 12 Plus (hasil data diolah)

Gambar 10 menunjukkan bahwa sudah banyak penelitian yang meneliti tanda tangan (*digital signature*). Validitas tanda tangan digital melalui proses verifikasi tanda tangan digital merupakan topik yang paling banyak dikaji. Secara umum semua penelitian yang meneliti topik verifikasi tanda tangan digital sebagian besar menyatakan aspek keamanan tanda tangan digital, termasuk penggunaan algoritma Message Digest 5 (MD5) (Precilia & Izzuddin, 2015), algoritma RSA (Ihwani, 2016), sertifikat digital pada tanda tangan digital (Perdana *et al.*, 2019), dan lainnya. Faktor keamanan perlindungan data menjadi prioritas untuk menjaga kerahasiaan, integritas, otentikasi entitas, dan otentikasi asal data.

Hasil analisis menggunakan perangkat lunak NVivo 12 Plus menunjukkan bahwa penggunaan tanda tangan digital (*digital signature*) untuk mengantisipasi kejahatan dunia maya (*cybercrime*) dalam mengimplementasikan kebijakan keamanan siber (*cybersecurity)* merupakan kebutuhan yang mendesak bagi pemerintah. Hal tersebut sejalan dengan konsep *smart governance* yang mengedepankan kebijakan *cybersecurity* dengan penerapan tanda tangan digital untuk mengantisipasi manipulasi data dan dokumen resmi yang dikeluarkan pemerintah sehingga proses tata kelola menjadi efektif, efisien, dan akuntabel.

5. Kesimpulan

Tanda tangan digital sebagai model penerapan kebijakan keamanan siber dalam penerapan *smart governance* merupakan kebijakan yang dibutuhkan oleh pemerintah dalam mengantisipasi kejahatan siber. Analisis menggunakan hasil software NVivo 12 Plus, sebagai berikut: 1) *Smart governance*, sebagai bagian dari *smart city*, memerlukan penerapan kebijakan penggunaan sertifikat elektronik. 2) Keamanan siber (*cybersecurity*) merupakan kebijakan yang harus dilakukan oleh pemerintah untuk mengantisipasi ancaman kejahatan siber (*cybercrime*). 3) Penggunaan tanda tangan digital (*digital signature*) sebagai bentuk baru penyelenggaraan *smart governance* dinilai sebagai kebijakan yang tepat oleh banyak pihak. Berdasarkan hasil analisis dengan menggunakan perangkat lunak NVivo 12 Plus, bentuk baru penyelenggaraan *smart governance* dalam penerapan tanda tangan digital, diperlukan untuk mengantisipasi ancaman *cybercrime* dalam melaksanakan pelayanan publik yang efektif, efisien, dan akuntabel.

https://doi.org/10.33019/society.v8i2.222

6. Ucapan Terima Kasih

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada pihak-pihak yang telah berkenan bekerjasama selama penelitian ini.

7. Pernyataan *Conflicts of Interest*

Penulis menyatakan tidak ada potensi konflik kepentingan sehubungan dengan penelitian, kepengarangan, dan/atau publikasi dari artikel ini.

Daftar Pustaka

Abraham, F. Z., Santosa, P. I., & Winarno, W. W. (2018). Tandatangan Digital Sebagai Solusi Teknologi Informasi dan Komunikasi (TIK) Hijau: Sebuah Kajian Literatur (Digital Signature as Green Information and Communication Technology (ICT) Solution: A Review Paper). *Masyarakat Telematika Dan Informasi: Jurnal Penelitian Teknologi Informasi dan Komunikasi*, *9*(2), 111-124. http://dx.doi.org/10.17933/mti.v9i2.120

Ahmad, D., Putri, D. A., Styawan, H., Nugraha, L. K., & Magdalena, M. (2018). *Kebijakan Cyber Security Dalam Perspektif Multi Stakeholder*. Jakarta, Indonesia: Kementerian Komunikasi dan Informatika Republik Indonesia.

Chyan, P. (2018). Penerapan sistem kriptografi enkripsi jamak dan tanda tangan digital dalam mendukung keamanan informasi. *TEMATIKA: Journal of Informatics and Information Systems*, *6*(1), 39-46. Retrieved from https://www.uajm.ac.id/files/journals/2/articles/83/submission/copyedit/83-156-1-CE.pdf

Darmayani, A. (2018). *SIBERPEDIA: Panduan Pintar Keamanan Siber*. Yogyakarta, Indonesia: Center for Digital Society, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Gadjah Mada.

Febrianta, M., Indrawati, I., & Amani, H. (2019, June 29). Identification of e-Governance Indicators for Measuring Smart Governance in Bandung City. https://doi.org/10.31227/osf.io/avbsu

Google Consumer Barometer. (2017a). *Do People Use The Internet For Personal Puposes*. Google Consumer Barometer. Retrieved from https://www.consumerbarometer.com/en/graph-builder/?question=N1&filter=country:indonesia

Google Consumer Barometer. (2017b). *How Often Do People Go Online (For Personal Internet Usage)*. Google Consumer Barometer. Retrieved from https://www.consumerbarometer.com/en/graph-builder/?question=M6&filter=country:indonesia

Google Consumer Barometer. (2017c). *Which Device Do People Use*. Google Consumer Barometer. Retrieved from https://www.consumerbarometer.com/en/graph-builder/?question=M1&filter=country:indonesia

Ihwani, M. (2016). Model Keamanan Informasi Berbasis Digital Signature Dengan Algoritma RSA. *Journal of Computer Engineering, Science and System*, *1*(1), 15-20. https://doi.org/10.24114/cess.v1i1.4037

Kumar, T. V. M. (2015). *E-Governance for Smart Cities*. Singapore: Springer Science+Business Media. https://doi.org/10.1007/978-981-287-287-6

Liyanti, L., & Hakim, A. R. (2019). Perancangan Penerapan Tanda Tangan Digital Sebagai Pengembangan Sistem Pelayanan Pentashihan Al Quran Digital. *SISTEMASI: Jurnal Sistem Informasi*, *8*(1), 41–54. https://doi.org/10.32520/stmsi.v8i1.415

Menezes, A. J., Oorschot, P. V. C., & Vanstone, S. A. (1997). *Handbook of Applied Cryptography (Discrete Mathematics and Its Applications)*. Florida, United States: CRC Press.

Miraz, M. H., Ali, M., Excell, P. S., & Picking, R. (2015). A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). *2015 Internet Technologies and Applications (ITA)*, 219–224. Wrexham, UK. https://doi.org/10.1109/itecha.2015.7317398

Munir, R. (2015). Penggunaan Tanda-Tangan Digital untuk Menjaga Integritas Berkas Perangkat Lunak. *Prosiding SNATi2015*, F-31-F-34. Yogyakarta, Indonesia. Retrieved from https://journal.uii.ac.id/Snati/article/view/1364

Pande, D. J. (2017). *Introduction to Cyber Security*. Uttarakhand, India: Uttarakhand Open University.

Perdana, R. A., Anbiya, D. R., & Grahitandaru, A. (2019). Penerapan Tanda Tangan Digital pada Gambar Formulir C1.Plano-KWK di Pilkada Sulawesi Selatan. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *6*(5), 475–484. https://doi.org/10.25126/jtiik.2019651471

Pooja, M., & Yadav, M. (2018). Digital Signature. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *3*(6), 71-75. Retrieved from http://ijsrcseit.com/paper/CSEIT183613.pdf

Precilia, D. P., & Izzuddin, A. (2015). Aplikasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritma Message Digest 5 (MD5). *Energy*, *5*(1), 14-19. Retrieved from https://ejournal.upm.ac.id/index.php/energy/article/view/155

Selular.id. (2018, August 5). Penggunaan Tanda Tangan Digital di Indonesia Tumbuh Pesat. Retrieved from https://selular.id/2018/08/penggunaan-tanda-tangan-digital-di-indonesia-tumbuh-pesat/

Septianingrum, A., Ahmad, D., Styawan, H., Ashar, I. M., Banyumurti, I., Mardiana, Magdalena, M., Ameliah, R., & Khoiriyah, R. (2018). *Pengantar Tata Kelola Internet*. Jakarta, Indonesia: Kementerian Komunikasi dan Informatika Republik Indonesia.

Tentang Penulis

1. **Nursani Budiarti,** mahasiswa pascasarjana Magister Ilmu Pemerintahan, Jusuf Kalla School of Government, Universitas Muhammadiyah Yogyakarta, Indonesia.
   E-Mail: nursani.budiarti@gmail.com

2. **Yahya Pandega Putra,** mahasiswa pascasarjana Magister Ilmu Pemerintahan, Jusuf Kalla School of Government, Universitas Muhammadiyah Yogyakarta, Indonesia.
   E-Mail: namakuyahya@gmail.com

3. **Achmad Nurmandi,** memperoleh gelar Doktor dari Universitas Indonesia pada tahun 2008. Penulis adalah Guru Besar pada Program Studi Politik Islam - Ilmu Politik, Jusuf Kalla School of Government, Universitas Muhammdiyah Yogyakarta, Indonesia.
   E-Mail: nurmandi_achmad@umy.ac.id

https://doi.org/10.33019/society.v8i2.222