Evaluasi Permasalahan Validasi Sertifikat TLS pada Domain Publik Indonesia

Vandega Arozan Musholine - 18223010
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail: 18223010@std.stei.itb.ac.id, egaarozan20@gmail.com

Abstrak—Transport Layer Security (TLS) adalah mekanisme kriptografi utama pada HTTPS, tetapi keamanan koneksi web tetap bergantung pada sertifikat digital yang disajikan server. Makalah ini mengevaluasi validasi sertifikat TLS pada domain publik Indonesia dengan pendekatan pengukuran yang aman dan mudah dipahami. Dari 167 kandidat awal, 77 hostname lolos proses canonicalization tanpa asumsi manual, lalu 75 hostname berhasil menyajikan sertifikat TLS dan menjadi sampel akhir. Metadata yang diamati meliputi status validasi, masa berlaku, kecocokan hostname terhadap Subject Alternative Name, penerbit sertifikat, algoritma tanda tangan, jenis public key, dan versi TLS. Hasil menunjukkan bahwa seluruh 75 sertifikat pada sampel akhir valid pada waktu pengujian. Tidak ditemukan expired certificate, hostname mismatch, self-signed certificate, atau untrusted CA. Kontribusi makalah ini adalah rancangan pipeline pengukuran, implementasi pengambilan metadata sertifikat, dan analisis empiris yang menjelaskan kondisi sertifikat TLS pada sampel domain publik Indonesia secara transparan.

Kata kunci—sertifikat digital; TLS; HTTPS; X.509; PKI; SAN; domain Indonesia; validasi sertifikat

I. PENDAHULUAN

Ketika pengguna membuka sebuah situs melalui HTTPS, browser biasanya menampilkan ikon gembok. Bagi pembaca awam, ikon tersebut sering dianggap sebagai tanda bahwa situs sudah aman sepenuhnya. Dalam kenyataannya, ikon tersebut terutama menunjukkan bahwa koneksi TLS dapat dibangun dan sertifikat digital yang diberikan server berhasil diverifikasi. Artinya, browser memiliki alasan kriptografis untuk percaya bahwa public key yang digunakan dalam koneksi memang terikat pada nama domain yang sedang dikunjungi.

Sertifikat TLS bekerja seperti kartu identitas digital untuk sebuah situs. Di dalamnya terdapat nama domain, public key, masa berlaku, penerbit sertifikat, dan tanda tangan digital dari Certificate Authority. Browser akan memeriksa apakah sertifikat masih berada dalam masa berlaku, apakah nama domain yang dibuka tercantum pada Subject Alternative Name, serta apakah rantai kepercayaannya berakhir pada pihak yang terdapat di trust store. Jika salah satu pemeriksaan dasar ini gagal, browser dapat menampilkan peringatan seperti koneksi tidak privat.

Masalah validasi sertifikat berbeda dari kerentanan aplikasi web seperti SQL injection atau Cross-Site Scripting. Penelitian ini tidak menilai apakah halaman web memiliki celah aplikasi, melainkan menilai apakah sertifikat TLS yang disajikan server dapat dipercaya oleh client pada saat koneksi dibuat. Ruang lingkup ini lebih sempit, tetapi penting, karena autentikasi server adalah dasar dari keamanan HTTPS.

Makalah ini membahas domain publik Indonesia karena domain tersebut banyak digunakan oleh masyarakat untuk mengakses informasi pemerintahan, pendidikan, bisnis, sekolah, dan layanan umum. Agar hasil tidak didasarkan pada perkiraan manual, penelitian menyaring kandidat domain melalui proses canonicalization antara bentuk root dan www. Setelah itu, program pengukur mengambil metadata sertifikat TLS secara sekuensial dan tidak agresif.

Kontribusi makalah ini terdiri dari tiga bagian. Pertama, rancangan pipeline yang menjelaskan perubahan dari kandidat awal menjadi sampel akhir. Kedua, implementasi pengambilan metadata sertifikat TLS melalui koneksi HTTPS standar. Ketiga, eksperimen terhadap 75 hostname final yang menghasilkan ringkasan validasi, penerbit sertifikat, masa berlaku, parameter kriptografi, dan versi TLS.

II. DASAR TEORI

A. TLS, sertifikat digital, dan Web PKI

Transport Layer Security atau TLS adalah protokol kriptografi yang digunakan untuk mengamankan komunikasi jaringan. Pada web, TLS digunakan oleh HTTPS untuk menjaga kerahasiaan data, integritas data, dan autentikasi *server*. Kerahasiaan berarti isi komunikasi tidak mudah dibaca pihak ketiga. Integritas berarti perubahan data dapat terdeteksi. Autentikasi *server* berarti *client* dapat memeriksa bahwa *server* yang dihubungi benar-benar mewakili domain yang dituju [1], [2].

Public Key Infrastructure atau PKI adalah infrastruktur kepercayaan yang mengatur penerbitan dan validasi sertifikat digital. Dalam konteks web publik, istilah yang lebih spesifik adalah *Web Public Key Infrastructure*. Web PKI melibatkan browser, sistem operasi, *Certificate Authority*, *root* certificate,

intermediate certificate, dan sertifikat TLS milik *server*. Browser dapat mempercayai suatu sertifikat karena rantai sertifikatnya tersambung ke *root* CA yang sudah ada di *trust store* [1].

Secara sederhana, hubungan kepercayaan tersebut dapat dibaca sebagai berikut: domain menyajikan sertifikat, sertifikat ditandatangani oleh *Certificate Authority*, dan browser mempercayai *Certificate Authority* tersebut. Jika seluruh pemeriksaan valid, browser dapat melanjutkan koneksi HTTPS tanpa peringatan.

B. Pemeriksaan utama pada sertifikat TLS

Validasi sertifikat TLS tidak hanya berarti mengecek apakah file sertifikat ada. Validasi mencakup beberapa pemeriksaan dasar. Pertama, waktu pengujian harus berada di antara *notBefore* dan *notAfter*. Kedua, *hostname* yang diakses harus tercantum dalam *Subject Alternative Name*. Ketiga, sertifikat harus diterbitkan oleh *Certificate Authority* yang dipercaya. Keempat, tanda tangan digital dan *public key* harus memakai parameter yang dapat diterima *client* modern [1], [3].

Rumus sederhana yang digunakan untuk menampilkan proporsi hasil adalah:

$$Presentasi\ kategorii\ = \frac{jumlah\ hostname\ pada\ kategori}{jumlah\ hostname\ sampel\ akhir}\ \times\ 100\%$$

Rumus tersebut penting karena penyebut harus jelas. Dalam makalah ini, persentase hasil validasi dihitung dari 75 *hostname* sampel akhir, bukan dari 167 kandidat awal. Alasannya, hanya 75 *hostname* tersebut yang benar-benar berhasil menyajikan sertifikat TLS dan dapat diperiksa.

TABLE I. RANCANGAN SAMPEL DOMAIN PUBLIK INDONESIA

Kelompok fitur	Contoh data	Fungsi analisis
Identitas sertifikat	subject, issuer	Menjelaskan identitas dan penerbit sertifikat.
Validitas waktu	notBefore, notAfter	Menilai apakah sertifikat masih berlaku.
Kecocokan domain	SAN, hostname match	Memastikan sertifikat cocok dengan domain yang dibuka.
Parameter kriptografi	public key, signature algorithm	Meringkas jenis kunci dan tanda tangan digital.
Koneksi TLS	TLS version, cipher suite	Menjelaskan koneksi yang berhasil dinegosiasikan.

III. METODOLOGI

A. Sumber kandidat dan pemilihan hostname

Dataset awal berisi 167 kandidat domain publik Indonesia. Kandidat tersebut dibagi ke dalam lima kategori, yaitu .go.id, .ac.id, .sch.id, .co.id, dan .id umum. Daftar awal tidak langsung dijadikan sampel akhir karena satu institusi dapat memakai bentuk domain berbeda, misalnya domain *root*, subdomain *www*, atau *redirect* ke *hostname* lain.

Agar pemilihan tidak bergantung pada asumsi pribadi, penelitian menguji dua bentuk alamat untuk setiap kandidat: https://domain dan https://*www*.domain. Program mencatat *final URL*, final host, status *redirect*, dan aturan pemilihan. Hostname hanya lolos otomatis jika bukti teknisnya cukup, misalnya salah satu bentuk aktif atau ada *redirect* yang jelas ke *hostname* final. Kandidat ambigu tidak dipaksa masuk agar hasil tidak menimbulkan kesalahan seperti *hostname mismatch* palsu.

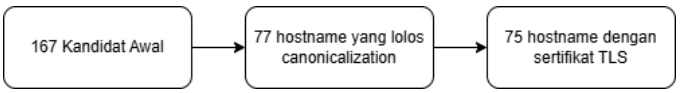


Fig. 1. Pipeline penyaringan sampel dan pengambilan metadata TLS.

Dari 167 kandidat awal, 77 *hostname* lolos *canonicalization* tanpa asumsi. Dari 77 *hostname* tersebut, 75 berhasil menyajikan sertifikat TLS. Dua *hostname* lain gagal pada tahap koneksi HTTPS sebelum sertifikat dapat diamati, sehingga tidak dihitung sebagai masalah validasi sertifikat. Pemisahan ini penting karena kegagalan mengambil data tidak sama dengan bukti bahwa sertifikatnya buruk.

B. Alur pengumpulan dan validasi

Pengambilan data dilakukan dengan koneksi HTTPS standar ke *port* 443. Program berjalan sekuensial, menggunakan *timeout*, dan memberi jeda antar *hostname*. Tidak ada *parallel scanning*, *brute force*, *fuzzing*, pengujian login, scraping konten, atau pemindaian *port* lain. Data yang dibaca hanya metadata sertifikat yang memang dikirim *server* dalam proses TLS *handshake*.

Metadata yang disimpan mencakup *hostname* final, kategori domain, waktu pengujian dalam WIB, versi TLS, *cipher suite*, *issuer*, masa berlaku, sisa hari menuju *notAfter*, *Subject Alternative Name*, hasil *hostname* match, *signature algorithm*, *public key* type, *public key* size, dan problem category. Dengan cara ini, pembaca dapat menelusuri angka pada tabel hasil kembali ke data dasar.

Karena penelitian ini berupa *snapshot*, seluruh klaim hasil hanya berlaku pada waktu pengujian. Sertifikat TLS dapat diperbarui, dipindah ke CA lain, atau berubah konfigurasinya pada hari berikutnya. Oleh karena itu, waktu pengujian perlu dicatat agar interpretasi hasil tetap adil.

TABLE II. KOMPOSISI SAMPEL AKHIR BERDASARKAN KATEGORI DOMAIN

Kategori	Jumlah	Persentase
.go.id	11	14,7%
.ac.id	17	22,7%
.sch.id	17	22,7%
.co.id	18	24,0%
.id umum	12	16,0%
Total	75	100,0%

C. *Aturan klasifikasi*

Klasifikasi masalah dibuat sederhana agar mudah dipahami. Sertifikat dinilai valid jika koneksi HTTPS berhasil, validasi default *client* berhasil, *hostname* cocok dengan SAN, dan sertifikat bukan *self-signed*. Jika sertifikat berhasil dibaca tetapi sudah melewati *notAfter*, kategorinya adalah *expired certificate*. Jika nama domain tidak tercakup dalam SAN, kategorinya adalah *hostname mismatch*. Jika validasi gagal karena CA tidak dipercaya, kategorinya adalah *untrusted CA* atau *self-signed*.

TABLE III. ATURAN SPESIFIKASI HASIL VALIDASI

Kategori	Aturan umum
Valid	HTTPS aktif, hostname cocok, dan sertifikat dipercaya client.
Expired certificate	Sertifikat berhasil dibaca tetapi melewati notAfter.
Hostname mismatch	Hostname yang diuji tidak tercakup dalam SAN.
Untrusted/self-signed	Validasi gagal karena CA tidak dipercaya atau sertifikat ditandatangani sendiri.
HTTPS unavailable	Koneksi TLS gagal sebelum sertifikat dapat dianalisis.

IV. HASIL DAN PEMBAHASAN

A. *Sumber kandidat dan pemilihan hostname*

Hasil utama eksperimen menunjukkan bahwa seluruh 75 sertifikat pada sampel akhir berstatus valid pada waktu pengujian. Tidak ditemukan *expired certificate*, *hostname mismatch*, *self-signed* certificate, atau *untrusted CA*. Untuk pembaca awam, hasil ini berarti semua situs yang masuk sampel akhir berhasil memberikan sertifikat yang dapat diterima browser secara dasar.

Namun, hasil tersebut tidak boleh dibaca sebagai klaim bahwa seluruh domain Indonesia pasti aman. Pertama, sampel akhir hanya berisi *hostname* yang berhasil disaring dan diamati sertifikatnya. Kedua, validitas sertifikat TLS hanya membuktikan bahwa hubungan antara *hostname* dan *public key* dapat diverifikasi. Validitas ini tidak membuktikan bahwa aplikasi web bebas malware, bebas phishing, atau bebas celah keamanan aplikasi.

TABLE IV. RINGKASAN KATEGORI VALIDASI PADA SAMPEL AKHIR

Kategori	Jumlah	Persentase
Valid	75	100,0%
Expired certificate	0	0,0%
Hostname mismatch	0	0,0%
Self-signed/untrusted CA	0	0,0%

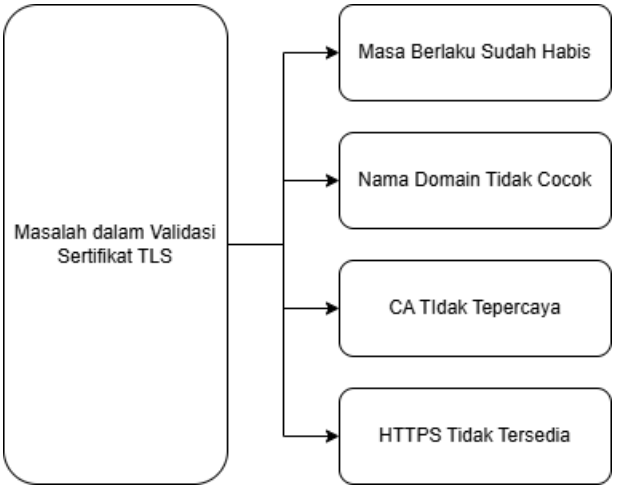


Fig. 2. Taksonomi masalah validasi sertifikat TLS dan posisi hasil penelitian.

B. *Penerbit sertifikat*

Penerbit sertifikat atau *issuer* menunjukkan *Certificate Authority* yang menandatangani sertifikat. Analisis *issuer* tidak dimaksudkan untuk menyatakan satu CA pasti lebih aman daripada CA lain. Selama sertifikat valid dan dipercaya browser, CA yang berbeda dapat sama-sama berfungsi dalam Web PKI. Analisis ini berguna untuk melihat ketergantungan sampel pada beberapa CA publik besar.

Pada sampel akhir, DigiCert Inc muncul sebanyak 24 sertifikat, diikuti Let's Encrypt sebanyak 20, Sectigo Limited sebanyak 14, dan Google Trust Services sebanyak 11. Sisanya berasal dari GlobalSign nv-sa, GoDaddy.com, ZeroSSL GmbH, dan Amazon. Distribusi ini menunjukkan bahwa domain pada sampel menggunakan CA yang umum ditemukan pada ekosistem web publik.

TABLE V. RINGKASAN ISSUER ORGANIZATION

Issuer	Jumlah	Persentase
DigiCert Inc	24	32,0%
Let's Encrypt	20	26,7%
Sectigo Limited	14	18,7%
Google Trust Services	11	14,7%
GlobalSign nv-sa	3	4,0%
Lainnya	3	4,0%

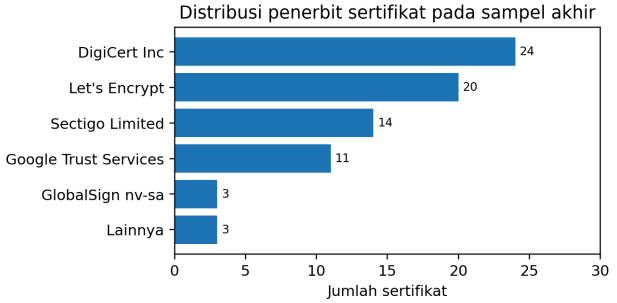


Fig. 3. Distribusi issuer organization pada sampel akhir.

C. Masa berlaku sertifikat

Masa berlaku sertifikat dibaca dari field *notBefore* dan *notAfter*. Sertifikat valid hanya jika waktu pengujian berada di dalam rentang tersebut. Pada sampel akhir, sisa masa berlaku minimum adalah 23 hari, median 84 hari, dan maksimum 280 hari. Tidak ada sertifikat yang kedaluwarsa pada saat data dikumpulkan.

Walaupun tidak ada sertifikat yang bermasalah, masa berlaku tetap penting secara operasional. Terdapat 2 sertifikat dengan sisa masa berlaku paling banyak 30 hari, 23 sertifikat paling banyak 60 hari, dan 42 sertifikat paling banyak 90 hari. Kelompok ini bukan kegagalan kriptografi, tetapi menjadi tanda bahwa pengelola domain perlu memiliki *monitoring* agar pembaruan sertifikat tidak terlewat.

TABLE VI. RINGKASAN SISA MASA BERLAKU SERTIFIKAT

Indikator	Nilai	Makna
<= 30 hari	2	Perlu dipantau lebih dekat.
<= 60 hari	23	Masih valid, tetapi mendekati jadwal pembaruan.
<= 90 hari	42	Mayoritas berada pada siklus pembaruan pendek.
Median	84 hari	Nilai tengah sisa masa berlaku.

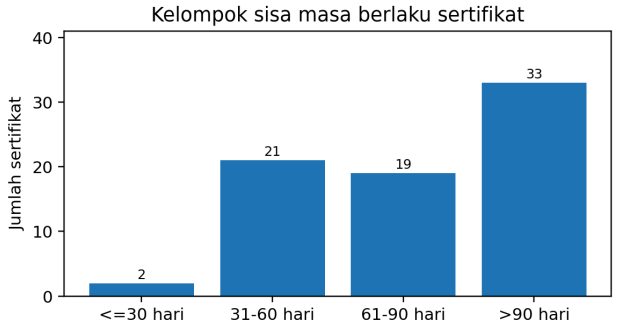


Fig. 4. Kelompok sisa masa berlaku sertifikat pada sampel akhir.

D. SAN, versi TLS, dan parameter kriptografi

Seluruh 75 *hostname* pada sampel akhir memiliki *hostname* match bernilai benar. Artinya, nama domain yang diuji tercakup dalam *Subject Alternative Name* pada sertifikat. Hasil ini menunjukkan bahwa proses *canonicalization* membantu menghindari kesalahan pengukuran. Jika penelitian langsung memakai *root* domain padahal situs resmi berpindah ke *www*, hasilnya dapat keliru terlihat sebagai *hostname mismatch*.

Dari sisi koneksi, 66 *hostname* menggunakan TLSv1.3 dan 9 *hostname* menggunakan TLSv1.2. Keduanya masih dapat diterima dalam konteks koneksi modern, meskipun TLSv1.3 memiliki desain yang lebih baru. Public key didominasi RSA sebanyak 56 sertifikat, sedangkan EC muncul pada 19 sertifikat. Signature algorithm yang paling banyak ditemukan adalah sha256 sebanyak 66 sertifikat.

TABLE VII. RINGKASAN PARAMETER TEKNIS TLS DAN SERTIFIKAT

Aspek	Nilai utama	Jumlah
TLS version	TLSv1.3 / TLSv1.2	66 / 9
Public key type	RSA / EC	56 / 19
Signature algorithm	sha256 / sha384 / sha512	66 / 8 / 1
Hostname match	True	75 dari 75

V. DISKUSI UMUM

Temuan seluruhnya valid dapat dibaca dari dua sisi. Sisi positifnya, domain yang lolos seleksi dan berhasil menyajikan sertifikat menunjukkan praktik TLS yang baik pada sampel akhir. Browser dapat memverifikasi identitas TLS *server* untuk *hostname* tersebut. Bagi pengguna, kondisi ini mengurangi risiko peringatan sertifikat dan membantu menjaga kepercayaan saat mengakses layanan publik.

Sisi lainnya, hasil ini harus dibatasi secara metodologis. Penelitian tidak mengevaluasi semua domain Indonesia. Penelitian juga tidak mengevaluasi keamanan aplikasi web, keamanan *server* secara menyeluruh, kebijakan privasi, atau konten halaman. Sertifikat yang valid hanya menunjukkan bahwa autentikasi TLS dasar berhasil. Karena itu, kesimpulan makalah tidak boleh diperluas menjadi klaim bahwa seluruh situs dalam sampel bebas risiko keamanan.

Keputusan menggunakan 75 sampel akhir lebih jujur daripada memaksa jumlah 100. Dari 167 kandidat awal, hanya 77 yang lolos *canonicalization* otomatis tanpa asumsi. Dari 77 itu, 75 menyajikan sertifikat yang dapat dibaca. Memaksa jumlah bulat dapat memasukkan *hostname* ambigu dan membuat hasil terlihat rapi tetapi kurang dapat dipertanggungjawabkan.

Bagi pengelola domain, pelajaran utamanya adalah validitas sertifikat perlu diperlakukan sebagai proses operasional, bukan pekerjaan sekali pasang. Domain perlu memiliki daftar aset, tanggal kedaluwarsa sertifikat, CA penerbit, *server* tempat sertifikat dipasang, dan penanggung jawab teknis. Tanpa inventaris dan *monitoring*, sertifikat yang hari ini valid dapat berubah menjadi *expired certificate* pada periode berikutnya.

VI. KETERBATASAN DAN ETIKA PENGUKURAN

Penelitian ini bersifat cross-sectional *snapshot*. Data diambil satu kali, sehingga hasil hanya menggambarkan kondisi pada waktu pengujian. Jika pengukuran diulang pada hari lain, *issuer*, valid_until, *cipher suite*, atau TLS version dapat berubah. Perubahan tersebut tidak selalu berarti penelitian sebelumnya salah, tetapi menunjukkan bahwa ekosistem TLS bersifat dinamis.

Penelitian ini juga tidak mengevaluasi revocation melalui OCSP atau CRL, tidak melakukan audit *Certificate Transparency* secara mendalam, tidak memeriksa konfigurasi HTTP security header, dan tidak melakukan uji penetrasi aplikasi. Batasan ini sengaja dipilih agar fokus makalah tetap pada validasi sertifikat TLS yang dapat diamati melalui *handshake* standar.

Dari sisi etika, proses pengukuran hanya melakukan koneksi HTTPS standar ke *port* 443, berjalan sekuensial, memakai

timeout, dan diberi jeda antar *hostname*. Penelitian tidak melakukan eksploitasi, autentikasi, *brute force*, *fuzzing*, *parallel scanning*, atau pengambilan konten sensitif. Hasil yang disajikan juga bersifat agregat agar tidak mengekspos institusi tertentu secara tidak perlu.

VII. REKOMENDASI

Walaupun sampel akhir tidak menunjukkan masalah validasi, beberapa rekomendasi tetap relevan untuk mencegah masalah di masa depan. Rekomendasi ini tidak hanya bersifat teknis, tetapi juga tata kelola. Sertifikat TLS adalah bagian dari Web PKI, sehingga keberhasilannya bergantung pada kombinasi konfigurasi *server*, proses pembaruan, dan pencatatan aset domain.

TABLE VIII. REKOMENDASI PEMANTAUAN SERTIFIKAT TLS

Objek cek	Frekuensi	Tujuan
Sisa masa berlaku	Harian/mingguan	Mencegah sertifikat kadaluarsa tanpa disadari.
Kecocokan SAN	Saat domain berubah	Memastikan hostname baru tercakup sertifikat.
Issuer dan chain	Bulanan	Mendeteksi perubahan CA atau rantai sertifikat.
Domain root dan www	Bulanan	Mendeteksi perubahan canonical hostname.
Kegagalan HTTPS	Insidental	Membedakan gangguan sementara dan masalah menetap.

Pengelola domain juga sebaiknya menggunakan mekanisme *auto-renewal* jika sesuai, memasang *fullchain* certificate dengan benar, dan menetapkan penanggung jawab sertifikat. Untuk organisasi yang memiliki banyak domain, dashboard *monitoring* sederhana sudah cukup membantu karena masa berlaku sertifikat berada pada skala hari sampai bulan, bukan detik.

VIII. KETERBATASAN DAN PEKERJAAN LANJUTAN

Keterbatasan pertama adalah sifat temporal dari sertifikat *TLS*. Status sertifikat dapat berubah karena pembaruan otomatis, migrasi server, atau perubahan konfigurasi DNS. Karena itu, hasil evaluasi hanya merepresentasikan kondisi pada waktu pengambilan data. Pengujian ulang pada beberapa waktu berbeda dapat membantu membedakan masalah sementara dan masalah konfigurasi yang konsisten.

Keterbatasan kedua adalah perbedaan perilaku antar-klien. Browser, *library TLS*, dan sistem operasi dapat memiliki *trust store* serta kemampuan membangun *certificate chain* yang berbeda. Akibatnya, satu konfigurasi dapat terlihat valid pada satu klien tetapi gagal pada klien lain. Pekerjaan lanjutan dapat membandingkan hasil validasi dari beberapa klien, misalnya OpenSSL, NSS, dan sistem operasi yang berbeda.

Pekerjaan lanjutan juga dapat memasukkan analisis *Certificate Transparency*, DNS *CAA*, dan status pencabutan melalui *OCSP* atau *CRL*. Namun, variabel tambahan tersebut sebaiknya dipisahkan dari validasi dasar agar pembahasan tetap jelas dan tidak mencampur masalah identitas server dengan masalah kebijakan penerbitan sertifikat.

IX. KESIMPULAN

Makalah ini mengevaluasi permasalahan validasi sertifikat TLS pada domain publik Indonesia dengan pendekatan *measurement study* yang disederhanakan agar mudah dipahami. Dari 167 kandidat awal, 77 *hostname* lolos *canonicalization* tanpa asumsi, dan 75 *hostname* berhasil menyajikan sertifikat TLS. Seluruh analisis hasil dihitung dari 75 sertifikat yang benar-benar teramati.

Hasil eksperimen menunjukkan bahwa seluruh 75 sertifikat pada sampel akhir valid pada waktu pengujian. Tidak ditemukan *expired certificate*, *hostname mismatch*, *self-signed* certificate, atau *untrusted CA*. Issuer didominasi oleh DigiCert Inc, Let's Encrypt, Sectigo Limited, dan Google Trust Services. Sebagian besar koneksi menggunakan TLSv1.3, *public key* RSA, dan *signature algorithm* sha256.

Kontribusi utama penelitian ini adalah *pipeline* pemilihan *hostname* tanpa asumsi, implementasi pengambilan metadata sertifikat TLS secara aman, dan analisis empiris terhadap sampel domain publik Indonesia. Pengembangan berikutnya dapat menambahkan pengukuran berkala, audit certificate chain yang lebih rinci, pemeriksaan revocation, dan pemanfaatan *Certificate Transparency* untuk memperluas analisis Web PKI.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pengampu mata kuliah II4021 Kriptografi, yaitu Prof. Dr. Ir. Rinaldi, M.T., yang telah memberikan ilmu, baik terkait kriptografi maupun di luarnya, yang bermanfaat.

REFERENSI

[1] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile," RFC 5280, IETF, 2008.

[2] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, IETF, 2018.

[3] CA/Browser Forum, "Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates," CA/Browser Forum, 2026.

[4] B. Laurie, E. Messeri, and R. Stradling, "Certificate Transparency Version 2.0," RFC 9162, IETF, 2021.

[5] OWASP Foundation, "Transport Layer Security Cheat Sheet," OWASP Cheat Sheet Series, 2026.

[6] V. Le Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczynski, and W. Joosen, "Tranco: A research-oriented

top sites ranking hardened against manipulation," in Proc. NDSS, 2019.

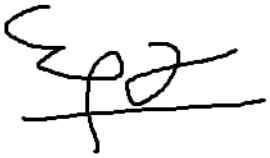
[7] A. P. Pelekoudas, E. Bolis, J. Lindner, P. Kyriakidis, M. Davidsen, J. T. E. Hansen, C. H. Reichkendler, and S. Homayoun, "TLS certificate and domain feature analysis of phishing domains in the Danish .dk namespace," arXiv:2603.21652, 2026.

[8] R. Holz, L. Braun, N. Kammenhuber, and G. Carle, "The SSL landscape: A thorough analysis of the X.509 PKI using active and passive measurements," in Proc. ACM IMC, 2011.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 19 Juni 2026



Vandega Arozan Musholine - 18223010