Jurnal Ilmiah Mustek Anim Ha Vol. 4 No. 2, Agustus 2015
ISSN 2089-6697

STUDI TENTANG PELUANG DAN TANTANGAN LAYANAN KRIPTOGRAFI BERBASIS CLOUD

Fransiskus Xaverius Manggau

Email : fransiskus@unmus.ac.id

Jurusan Teknik Informatika, Fakultas Teknik

Universitas Musamus Merauke

Abstrak

Penempatan kunci kriptografi pada *end point device* seperti smartphone dan aplikasi layanan publik akan menimbulkan resiko tersendiri. Peralatan tersebut umumnya menerapkan end point cryptography dan sangat rentan dengan vulnerabilitas serta dipandang sebagai bad place untuk menghasilkan key generator. Cloud adalah sebuah solusi yang banyak ditawarkan untuk mengatasi permasalahan tersebut. Dalam hal ini, Cryptography as a Service (CaaS) adalah salah satu teknik cloud yang dikembangkan untuk memberikan solusi adanya vulnerabilitas yang terjadi pada saat endpoint cryptography process. Tulisan ini memberikan studi tentang pendalaman issue CaaS melalui eksplorasi cara kerja serta potensi penerapan dan tantangan yang mungkin akan dihadapi dalam implementasinya. Penerepan pada end user mobile phone serta e-government adalah merupakan peluang dari implementasi CaaS. Solusi CaaS sebenarnya memberikan harapan akan kemudahan dalam mengimplementasikan kebutuhan teknologi kriptografi yang diperlukan oleh berbagai aplikasi yang dijalankan diatas perangkat end point. Namun demikian sejumlah issue security masih menjadi salah satu kendala yang harus diantisipasi kedepannya. Selain itu, penerapan kriptografi pada CaaS juga masih harus mempertimbangkan konsep “dual use” technology yang umumnya dikontrol penggunaannya oleh sejumlah negara.

Keywords: Kriptografi, Authentikasi, Cloud, CaaS, Dual Use

PENDAHULUAN

Keamanan adalah merupakan tuntutan dasar dari setiap pengguna agar dapat menjalankan berbagai aktivitas sehari-harinya berbantuan teknologi komputer. Dalam hal ini walaupun keamanan tidak sama dengan kriptografi, namun [1] tetap memandang bahwa komponen utama dari keamanan adalah kriptografi. Karena itu berbicara tentang masalah keamanan tidak lepas dari pembicaraan seputar kriptografi.

Sedemikian pentingnya kriptografi ini, maka sejumlah negara telah memiliki perangkat hukum dan perundangan yang

mengatur sejumlah regulasi tentang kriptografi. Sebagai contoh negara Amerika Serikat, memiliki aturan terkait dengan export atau import teknologi kriptografi, demikian juga dengan beberapa negara di Eropa dan China [1]. Sayangnya Indonesia tidak termasuk dalam negara yang sudah memiliki regulasi tentang kriptografi ini. Untuk kepentingan itulah maka saat ini pemerintah Indonesia melalui Lembaga Sandi Negara (Lemsaneg) sedang merumuskan sebuah RUU Persandian. Salah satu yang diantisipasi dari perumusan RUU tersebut adalah berkembangnya industri keamanan (baik perangkat keras maupun perangkat lunak) sebagai implementasi dari upaya untuk memberikan solusi kepada masyarakat terhadap masalah keamanan komputer.

Selanjutnya, menurut [1], negara-negara besar umumnya menerapkan regulasi yang berbeda terhadap teknologi kriptografi. Hal ini tidak lepas dari sifat teknik enskripsi dan dekripsi yang termasuk dalam katagori teknologi "*dual-use*", yaitu teknologi yang dapat bersifat komersial maupun militer. Selanjutnya untuk mengatur peredaran dari produk atau teknologi yang bersifat "dual use" tersebut, beberapa negara membuat perjanjian internasional, yang dikenal dengan Wassenaar Arrangement. (http://www.wassenaar.org/). Tujuan dari Wassenaar Arrangement adalah untuk mendorong transparansi dan tanggungjawab yang lebih besar dari tiap negara berkaitan dengan akuisisi, transfer, maupun akumulasi dari produk atau teknologi yang berjenis "dual use" tersebut.

Sementara itu, [1] menjelaskan bahwa salah satu contoh hal yang diatur dalam Wassenaar Arrangement adalah batasan panjang kunci yang bebas diekspor, yaitu 56 bit untuk symmetric cryptography dan 512 bit untuk asymmetric cryptography. Dengan demikian dibenarkan bila seseorang bepergian lintas negara dengan membawa alat kriptografi asalkan untuk kepentingan pribadi. Pada prinsipnya, setiap produk atau teknologi yang dianggap bersifat "*dual use*" harus diatur secara ketat pembuatan, penggunaan, dan ekspornya.

Issue kriptografi menjadi sebuah issue sensitif bila ternyata diberikan melalui layanan cloud. Hal ini sejalan dengan pakta dan tuntutan terhadap terjadinya pergeseran trend komputasi komputer,

mulai dari *client-server* menuju sistem terdistribusi dan saat ini sentralisasi secara virtual atau yang lebih dikenal dengan *cloud computing*. Dalam hal ini, sejalan dengan perkembangan cloud, dimana efisiensi biaya dapat ditekan dengan memanfaatkan layanan cloud, maka kini mulai tersedia sejumlah layanan yang mengarah pada memanfaatkan teknologi cloud untuk mengamankan data melalui Cryptography as a service (CaaS), atau Encryption as a Service (EaaS) atau Security as a Service (SecaaS).

Dalam kaitannya dengan issue RUU Persandian, maka ketersediaan layanan cloud untuk kriptografi adalah merupakan salah satu issue yang harus didalami. Salah satu kepentinganya adalah sifat dan karakteristik layanan cloud yang *borderless* dan membutuhkan pendekatan yurisdiksi lintas negara. Tentunya apabila teknologi kriptografi dapat dengan mudah didapat dan ditawarkan melalui layanan cloud maka hampir mustahil untuk melakukan pengawasan terhadap penggunaan teknologi kriptografi di masyarakat nantinya. Untuk itulah tulisan ini mencoba untuk membahas lebih lanjut seputar issue cryptography as a service dari aspek teknis dan konsep dasarnya serta peluang dan tantangan yang mungkin akan dihadapi dalam implemenyasinya.

Diantara beberapa pengertian dan model tentang Cryptography as a Service (CaaS) sebagaimana yang dikemukakan dalam [2]–[8], maka salah satu yang menarik untuk dikaji lebih lanjut adalah model CaaS yang dikembangkan oleh [7], [9]. Dalam hal ini [10] telah melakukan kajian tentang komparasi cara kerja CaaS dengan menerapkan perbandingan melalui mekanisme authentikasi protocol Kerberos. Secara detail [10] menjelaskan bahwa CaaS dan Kerberos sebenarnya adalah dua objek yang berbeda. CaaS fokusnya pada pemberian layanan cryptography berbasis pada cloud sementara Kerberos adalah merupakan sebuah protocol untuk authentikasi user dalam sebuah jaringan komputer. Namun diantara perbedaan antara CaaS dan Kerberos yang menarik adalah fungsi tiga mesin dalam CaaS (Cryptography Provider, Authentication Server dan Key Manager) ternyata memiliki kemiripin fungsi dengan peran Client, Server dan Server Kerberos (KDC) dalam Kerberos. Pada CaaS, ketiga mesin tersebut tersimpan lewat layanan cloud dan digunakan untuk menjalankan prosedur

authentikasi pengguna serta menggenerate dan menyimpan kunci kriptografi. Sementara dalam Kerberos, mesin tersebut berfungsi secara fisik dan digunakan untuk memproses mekanisme authentikasi antar device dalam sebuah jaringan.

Mengingat masih banyak aspek dari CaaS yang perlu dikaji lebih lanjut, maka paper ini ditulis dengan tujuan untuk mendalami lebih lanjut tentang peluang dan tantangan penerapan CaaS untuk berbagai keperluan implementasi teknologi informasi kedepannya.

GAMBARAN UMUM

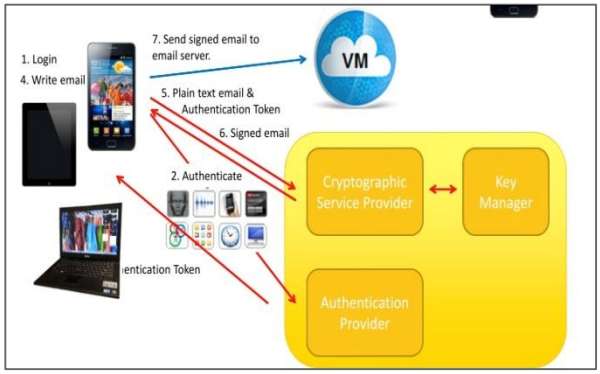
Definisi dan penerapan terminologi dari **cryptography as a service *(CaaS)*** itu sendiri masih belum seragam dan masih terdapat perbedaan pandangan antara satu peneliti dengan peneliti yang lain. Demikian juga antara peneliti dengan praktisi industri keamanan komputer. Dianatara definisi dan penerapan istilah tersebut adalah :

- CaaS sebagai *Communication as a service*. Terminologi ini dikemukakan oleh [4], yaitu sebuah layanan yang meliputi: *dedicated bandwidth*, *network security*, *encryption* dan *network monitoring*.
- CaaS sebagai *Cryptography as a service*. Terminologi ini dikemukan oleh sejumlah peneliti, antara lain: ([2],[11], [7], [6]. Maksudnya adalah membahas solusi keamanan komputer dalam skema cloud computing.
- Issue sejenis dengan dengan CaaS adalah *Encription as a Service* (EaaS) dikemukakan oleh [6] dan *Security as a Service* (SecaaS) yang dikemukakan oleh [8]. Kedua istilah terakhir ini lebih kepada bagaimana memberikan solusi keamanan pada *cloud provider* terutama melalui melalui pendekatan arsitektur sistem cloud.

Pembahasan selanjutnya akan difokuskan pada istilah Cryptography as a service, walaupun dalam beberapa aspek maknanya hampir memiliki kesamaan dengan Encryption as a Service (EaaS) maupun Security as a service (SecaaS). Pengertian Cryptography as a service itu sendiri masih belum sama dan terdapat beberapa makna dan penerapan yang berbeda. Secara garis besar terbagi menjadi 3 pengertian umum, yaitu : solusi kriptografi untuk layanan keamanan cloud computing, solusi kriptografi melalui layanan cloud provider dan solusi

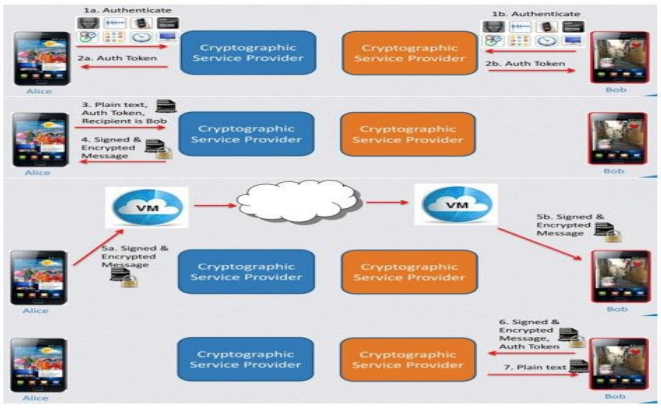
hardware melalui vitual HSM (*Hardware Security Module*).

Model CaaS yang diusulkan oleh [7], [9], pada prinsipnya adalah sebuah mekanisme: "*cryptographic operations on behalf of end points via web services*". Hal ini dapat dijelaskan sebagaimana pada ilustrasi Gambar 1.



Gambar 1 Ilustrasi Cara Kerja CaaS

CaaS dapat diterapkan antara lain untuk kepentingan penggunaan aplikasi email, melihat data terenkripsi yang tersimpan pada end point ataupun pada cloud dan melakukan sharing antar device. Dalam hal penggunaan aplikasi email, pemilik end point device dapat mengirimkan signed email dan menerima pesan terenkripsi melalui mekanisme CaaS. Ilustrasi dari penerapannya adalah sebagaimana pada Gambar 2.



Gambar 2 Ilustrasi Cara Kerja CaaS

Berdasarkan ilustrasi pada Gambar 1 dan 2, maka untuk penerapan CaaS pada aplikasi pengiriman email perangkat smartphone, langkah kerjanya adalah sebagai berikut:

1. Login aplikasi pada perangkat *end point*.
2. Proses strong authentification antara *end point* dengan layanan CaaS.
3. Bila berhasil maka didapat token authentification.
4. User menuliskan konten email yang akan dikirimkannya.
5. Plain Text email dan token authentification dikirimkan ke service provider.
6. Outputnya berupa signed email.
7. Signed Email selanjutnya dikirimkan oleh end point ke email server.

Selanjutnya, menurut [9], layanan CaaS hanya memerlukan authentikasi *end point* device untuk memastikan bahwa device tersebut memang dapat melakukan akses terhadap CaaS. Untuk itu maka perlu mekanisme yang ketat untuk melakukan authentikasi (*strong authentication*), proses ini dapat dilakukan melalui authentikasi user (*password,voice,facial recognition, motion based, one time password*) dan authentikasi environment (Device ID, SIM number, phone number, MAC Address, Location, Apps allowed to be on phone, Time of day). Tabel 1 menjelaskan bagaimana mekanisme yang dapat diterapkan untuk mendukung mekanisme *strong authentication*.

Semua operasi untuk menghasilkan kunci kriptografi dijalankan oleh CaaS provider melalui *Representational State Transfer* (REST) atau *Key Management Interoperability Protocol* (KMIP) yang berjalan diatas *Transport Layer Security* (TLS). Melalui solusi ini maka *end point device* (misalnya Handphone) tidak perlu menyimpan key didalam handphonenya namun tetap dapat mengirim dan menerima pesan yang terenkripsi, melihat data-data yang terenskripsi dalam handphonenya juga melihat data yang terenkripsi didalam cloud. Berdasarkan ilustrasi pada Gambar 2 tersebut maka hal penting dari mekanisme CaaS adalah sebagai berikut:

- Operasi pemberian kunci kriptografi (enkripsi dan dekripsi) dijalankan oleh provider CaaS atas nama end point melalui layanan API web.
- Tidak ada kunci kriptografi penting pada end points.
- Kunci kriptografi disimpan dan dibackup dalam satu tempat tertentu.
- Dilakukan mekanisme End Point Authentication untuk menjamin bahwa hanya end point yang terauthorisasi yang dapat menggunakan layanan CaaS.

Model CaaS yang diusulkan oleh ini [7], [9], diklaim memiliki sejumlah keuntungan, diantaranya adalah :

- Tanpa harus menyimpan kunci kriptografi pada end point (handphone misalnya) namun melalui CaaS memungkinkan end point untuk mengirim dan menerima message yang terenkripsi.
- Dapat melihat data data yang terenkripsi dalam end point device maupun pada cloud service lainnya.

- Dapat melakukan sentralisasi manajemen dan sharing data antar device.
- Dapat meningkatkan keamanan dan menutup celah vulnerabilitas.

Tabel 1 Mekanisme Strong Authentification

End Point Device	***Authentikasi***
Smartphone	• User: Password, Voice print, Facial recognition, Motion based, SecurId One Time Password. • Environment: Device: Device ID, SIM number, Phone number, Location, Apps allowed to be on phone, Time of day. • Services available depend on the degree to which the identity is authenticated. • Alternatively, perhaps the level of authentication could be "stepped-up" if the requested service requires a higher degree of authentication than has been provided.
Cloud / VM	• Mutually authenticated TLS: TLS Client private key must be stored on VM and protected. • Server authenticated TLS with a password or PIN: • Environment : • System values: Complex due to virtualization layer, and technologies such as vMotion • Virtual Trusted Platform Module (vTPM).
	• Software attestation / environmental comparison
Grid	• Device Unique Identifier. • MAC Address • Installation PIN

Namun demikian, terdapat pula sejumlah hal yang akan menjadi kelemahan dari CaaS, yaitu:

- Bertambahnya kompleksitas arsitektur
- Adanya kelambatan (Latency) karena harus melalui web calls.
- Dimungkinkan menurunnya performance karena meningkatnya overhead Karena melakukan web calls.
- Diperlukan tambahan hardware sebagai host untuk CaaS provider.
- Kemungkinan terjadinya Denial of Service karena adanya lost connection antara end point dengan provider CaaS ketika menjalankan operasi kriptografi.

Dengan berbagai kelebihan dan kekurangannya, CaaS sebenarnya diharapkan menjadi solusi bagi ketersediaan layanan kriptografi yang kuat tanpa harus menggunakan bantuan Hardware Security Module (HSM) atau sebuah crypto processor. Gambar 3 berikut ini adalah gambaran yang dharapkan dari penggunaan CaaS dan HSM [9].

CaaS	Hardware Security Module (HSM)
Scalability and on demand elastic scaling	Fixed scaling
Virtual Machine	Hardware
Higher Performance	Lower Performance
Wider API support / more flexible APIs KMIP, REST / Proprietary, (and PKCS #11)	Narrower API support / less flexible APIs PKCS #11, Proprietary, (and KMIP)
FIPS 140 Security Level 1 or 2	FIPS 140 Security Level 3 or 4
Lower cost	Higher cost

Gambar 3 Perbandingan Umum CaaS dan HSM

POTENSI PENERAPAN LAYANAN KRIPTOGRAFI BERBASIS CLOUD

Solusi CaaS yang ditawarkan oleh [7], [9], memang dilatarbelakangi oleh tuntutan kriptografi untuk *end point device*, salah satunya adalah handphone/ smartphone. Mengingat kecenderungan handphone saat ini sebagai alat komunikasi yang secara masif dimiliki oleh semua lapisan masyarakat, maka tentunya akan mengubah perilaku dan gaya hidup masyarakat itu sendiri. Karena itu maka ketersediaan sejumlah aplikasi mobile yang terinstall dalam perangkat handphone harus benar-benar didukung oleh teknologi yang benar-benar dapat memberikan jaminan keamanan bagi penggunanya.

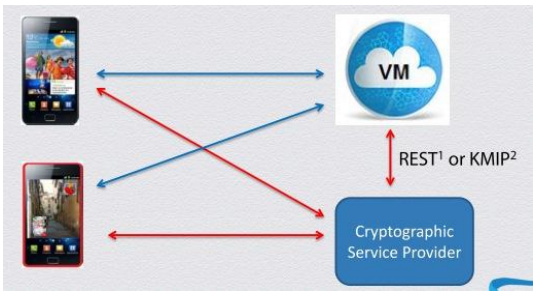
No.	Title	Risk
1	Data leakage resulting from device loss or theft	High
2	Unintentional disclosure of data	High
3	Attacks on decommissioned smartphones	High
4	Phishing attacks	Medium
5	Spyware attacks	Medium
6	Network Spoofing Attacks	Medium
7	Surveillance attacks	Medium
8	Diallerware attacks	Medium
9	Financial malware attacks	Medium
10	Network congestion	Low

Gambar 4. Resiko Keamanan untuk perangkat mobile

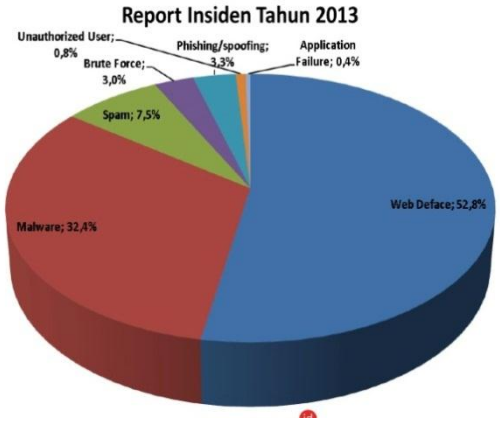
Terkait dengan security pada perangkat mobile, menurut [12], terdapat 10 resiko keamanan yang dapat terjadi pada perangkat mobile sebagaimana ilustrasi pada Gambar 4. Berdasarkan ilustrasi tersebut, maka resiko tertinggi sifatnya adalah non teknis. Resiko yang lain hanya akan mungkin terjadi bila aplikasi yang terinstal dalam perangkat mobile adalah berasal dari vendor yang tidak teriverifikasi dengan baik oleh system. Sementara resiko lainnya lebih pada resiko yang dihadapi sebagai konsekwensinya menggunakan jaringan telekomunikasi secara umum, maka enkripsi data untuk komunikasi maupun sharing data menjadi sangat penting.

Gambaran solusi yang diberikan oleh [7], [9] benar-benar memberikan harapan akan kemudahan dalam mengimplementasikan kebutuhan teknologi kriptografi yang diperlukan oleh berbagai aplikasi yang dijalankan diatas perangkat handphone. CaaS dapat

diterapkan untuk sejumlah kepentingan, yaitu : signed and ecrypted message, encrypted local data, encrypted cloud data, dan credential sharing. Dengan demikian solusi CaaS adalah merupakan solusi yang sangat potensial untuk diterapkan dalam teknologi kriptografi pada perangkat mobile kedepannya. Gambar 5 menunjukkan gambaran implementasi CaaS untuk mobile applications.



Gambar 5. Implementasi CaaS pada mobile application



Gambar 6 Statistik Incident terhadap situs pemerintah

Selain untuk kepentingan mendukung keamanan pada *end user* untuk pengguna handphone, maka CaaS juga dapat diterapkan untuk kepentingan layanan e-government. Dalam hal ini mengingat kompleksitas infrastruktur untuk layanan e-government, maka pengelola layanan kadang lebih memprioritaskan pada sistem dan konten layanan namun mengabaikan pada aspek keamanan. Hal ini dapat dipahami, karena umumnya untuk aspek keamanan ini diperlukan tenaga teknis yang lebih spesifik sementara ketersediaan tenaganya itu sendiri sangatlah terbatas. Karena itulah layanan e-gov sering menjadi para target attacker baik dari dalam maupun luar negeri. Data yang dikeluarkan oleh http://govcsirt.kominfo.go.id, menunjukkan bahwa upaya kearah attack terhadap situs pemerintah dan penyedia e-gov sepanjang tahun 2013 didominasi oleh web defacement (52.8 %) dan malware (32%). Karena itu menurut [13], penanganan keamanan e-gov yang paling penting adalah mengatasi vulnerabilitas web site melalui antisipasi terhadap aktivitas *Cross Site Scripting* (XSS) atau SQL injection.

Pada sisi lain, [14] melihat bahwa keamanan sebuah sistem e-gov harus didesain dalam sebuah framework yang melibat aspek non teknis dan teknis serta partisipasi aktif dari G-B-C (Government-business-citizen). Menurut pendapat Gartner, kematangan sistem keamanan sebuah e-gov terjadi dalam kurun waktu 5-10 tahun, dalam kurun waktu tersebut dapat dilihat peran aspek teknis dan non teknis dalam vulnerabilitas sistem e-gov sehingga dapat diberikan solusi terbaik kedepannya.

Penggunaan serta manfaat implementasi cloud untuk kepentingan e-gov telah dibahas oleh sejumlah peneliti, antara lain oleh [15] dan [16]. Pada prinsipnya untuk meningkatkan solusi sistem e-gov yang *reliable*, *economical* dan kemudahan maintenance, maka solusi cloud adalah pilihan yang tepat. Sementara issue keamanan pada implementasi cloud untuk e-gov lebih banyak membahas bagaimana teknik enkripsi data untuk menjamin confidentiality dan integritas data. [17]. Solusi cryptography as a service (CaaS) yang ditawarkan oleh [7], [9], maupun Cryptomathic dan Safenet, sangatlah potensial untuk diterapkan dalam lingkup layanan e-gov. Dalam implementasinya, sejumlah industri perbankan, yang memiliki ketergantungan sangat tinggi terhadap implementasi kriptografi, ternyata telah banyak memanfaatkan layanan Cryptomathic maupun Safenet.

ISSUE KEAMANAN PADA LAYANAN KRIPTOGRAFI BERBASIS CLOUD

Pada prinsipnya layanan yang ditawarkan oleh berbagai vendor ataupun peneliti terkait dengan issue *Cryptography as a Service* adalah sebuah solusi untuk menangkap peluang kebutuhan akan implementasi teknologi kriptografi saat ini. Sejauh ini belum ada kajian secara khusus yang membahas vulnerabilitas dari konsep cryptography as a service yang ditawarkan baik oleh [7], [9] maupun oleh vendor Crypthomathic dan CryptoHypervisor. Dengan asumsi bahwa konsep tersebut telah disiapkan secara matang oleh SDM yang sangat berpengalaman dalam bidang kriptografi, maka mestinya tidak ada kendala dari aspek jaminan keamanan untuk implementasinya.

Namun demikian, dari sisi aspek teknologi atau algoritma kriptografi, [18] menyebutkan bahwa pada prinsipnya

masalah yang dihadapi oleh kriptografi saat ini lebih pada pada aspek bagaimana mengatasi kelemahan pada saat implementasi yang mungkin tidak terduga sebelumnya. Dalam hal ini masalah keamanan tidak terletak hanya pada algoritma yang kuat saja namun juga pada penggunaan yang mudah namun aman dari sisi implementasinya. Hal inilah sebenarnya yang terjadi dengan kasus Snowden [19];[18], bocornya sejumlah informasi penting oleh Edward Snowden lebih pada memanfaatkan vulnerabilitas dari implementasi sistem keamanan bukan pada teknologi kriptografinya itu sendiri.

Walaupun demikian menurut [1], kekuatan sebuah sistem kriptografi tetap harus memperhatikan 3 faktor, yaitu key security yang menjadi tanggung jawab user, algoritma yang terbukti secara matematis akan kekuatannya serta key yang cukup panjang yang mustahil dipecahkan dengan brute-force attack. Dalam hal ini menurut Gartner dalam [2], terdapat 7 issue spesifik dalam bidang keamanan pada cloud computing, yaitu : *privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, long-term viability*. Sementara menurut , issue keamanan dalam cloud dapat dibagi dalam tiga katagori utama yaitu : Data Security, Data Storage Security dan Hostile Attack. Dalam hal ini [2] berpendapat, mengingat banyaknya ragam ancaman terhadap keamanan komputer maka hingga saat ini tidak ada yang bisa menjamin keamanan dalam bidang cloud computing ini.

Terkait dengan keamanan cloud computing, sejumlah pakar keamanan masih meragukan akan kehandalan keamanan dalam layanan cloud. Salah satunya adalah Ralph Spencer Poore, sebagaimana yang dilaporkan oleh [20]. Dalam laporan tersebut, Ralph Spencer Poore, salah seorang pakar cryptography menyebutkan bahwa : “"*In the cloud, we don't have the luxury of having actual, physical control over the storage of information, so the only way we can ensure that the information is protected is for it to be stored cryptographically, with us maintaining control of the cryptographic key*." Lebih lanjut Ralph Spencer Poore menyebutkan bahwa dalam urusan kriptografi dan keamanan sifatnya adalah *homeworks* dan sebaiknya tidak ikut terlena dengan berbagai imaginasi seputar solusi layanan cloud. Menurutnya,

masalah kriptografi adalah masalah yang sifatnya harus ditangani sendiri dan tidak termasuk dalam bagian yang harus diserahkan pada pihak lain (*outsourcing*). Pada bagian lain, Ralph Spencer Poore menyebutkan adanya issue lain yang cukup sensitif, yaitu masalah seputar yurisdiksi hukum. Layanan cloud cenderung sifatnya bersifat lintas negara sementara teknologi kriptografi itu sendiri pada sejumlah negara adalah teknologi yang dilindungi oleh hukum dengan sejumlah keterbatasan akses dan pemakaiannya. Aspek ini harus benar-benar dipahami oleh pengguna layanan cloud dan seharusnya termuat dalam ketentuan SLA yang disepakati dalam kontrak.

Namun demikian, Ralp Spencer Poore tidak sepenuh melarang memanfaatkan penggunaan cloud untuk urusan kriptografi, menurutnya kunci utamanya adalah pada bagaimana menerapkan konsep *management of cryptographic keys*, yaitu kontrol terhadap proses *encrypt* dan *decrypt* yang dilakukan oleh layanan cloud, serta kontrol terhadap konten dari kriptografinya itu sendiri. Pengguna harus mengenal dengan baik teknologi yang ditawarkan, serta kredibilitas penyedia layanannya. Selain itu juga harus ada seseorang yang memahami dengan baik aspek hukum dalam kontrak yang disepakati (SLA).

DISKUSI

Layanan CaaS sendiri masih belum sepenuhnya teruji terutama untuk mengatasi masalah networking, misalnya bila end point device tidak dapat terhubung dengan CaaS provider, juga masalah security tentang cache yang menyimpan kunci penting dan informasi tentang Authentikasi user. Dari sisi layanan cloud secara umum, tetap masih merupakan sebuah tantangan dalam hal keamanan walaupun menggunakan solusi private cloud. Tantangan keamanan lain untuk CaaS adalah bagaimana menjaga komunikasi antara end point dengan CaaS Provider selalu dalam skema trustworthy. Bila seorang attacker berhasil menguasai end point device dan lolos authentikasi service provider maka semua layanan yang tersedia dapat dikuasainya.

Terkait dengan keamanan cloud computing, sejumlah pakar keamanan masih meragukan akan kehandalan keamanan dalam layanan cloud. Salah satunya adalah Ralph Spencer Poore,

sebagaimana yang dilaporkan oleh [20]. Menurutnya, urusan kriptografi dan keamanan sifatnya adalah *homeworks* dan sebaiknya tidak ikut terlena dengan berbagai imaginasi seputar solusi layanan cloud. Masalah kriptografi adalah masalah yang sifatnya harus ditangani sendiri dan tidak termasuk dalam bagian yang harus diserahkan pada pihak lain (*outsourcing*). Layanan cloud cenderung sifatnya bersifat lintas negara sementara teknologi kriptografi itu sendiri pada sejumlah negara adalah teknologi yang dilindungi oleh hukum dengan sejumlah keterbatasan akses dan pemakaiannya. Aspek ini harus benar-benar dipahami oleh pengguna layanan cloud dan seharusnya termuat dalam ketentuan SLA (Service Level Agreement) yang disepakati dalam kontrak.

Dari aspek implementasi, solusi CaaS yang dikemukakan oleh Robinson masih belum direview, dikaji lebih lanjut, atau bahkan diimplementasikan secara langsung, tentunya berbeda dengan Kerberos yang telah banyak diadopsi dan diterapkan oleh berbagai vendor untuk berbagai keperluan mekanisme authentikasi user. Namun demikian, solusi CaaS ini sangatlah menarik mengingat faktanya adalah jumlah penguna mobile device yang semakin meningkat serta ketersediaan berbagai aplikasi pada platform inipun semakin luas dan variatif. Sehingga solusi CaaS sebenarnya adalah sebuah solusi yang sangat strategis.

Dari aspek keamanan, konsep CaaS sangat bergantung pada mekanisme untuk meyakinkan bahwa si pemilik *end point device* adalah benar-benar pemilik yang sah dari device tersebut sehingga memiliki kewenangan untuk melakukan akses kepada aplikasi. Untuk mendukung hal ini maka mekamisme yang diusulkan adalah menggunakan *strong authentication* pada end point device. Khususnya untuk ketersediaan layanan cloud, maka implementasi dari CaaS masih harus di lihat lebih lanjut berdasarkan mekanisme penerapan teknologi kriptografi sebagai layanan utama cloudnya. Permasalahan hukum dan yurisdiksi terhadap implementasi adalah hal yang belum dikaji lebih lanjut. Dari aspek infrastuktur, penerapan mesin *hardware security module* pada mesin kriptografinya serta konsep trusted computing yang mendasarinya juga masih menjadi topik yang perlu dikaji lebih lanjut. Selain itu issue yang masih perlu didalami adalah

tentang pemanfaatkan *Tranport Layer Security* (TLS) yang dijadikan sebagai media untuk komunikasi antara provider dengan *end point*.

Sementara itu terkait dengan konsekwensi penggunaan kriptografi dalam layanan cloud computing, maka issue yang juga harus dikaji lebih lanjut adalah ketentuan masalah yurisdiksi antar negara untuk penggunaan kriptografi pada layanan cloud. Menurut [21], bagi penegak hukum dan komunitas keamanan nasional, kontrol terhadap eksport kriptografi adalah merupakan kebijakan penting untuk mengatasi aktivitas kejahatan internasional dan terorisme. Karena itu adalah hal yang wajar apabila kemudian negara seperti Amerika Serikat menerapkan kebijakan yang sangat ketat dan berbagai regulasi sebagai kontrol bagi ekspor produk dan teknologi kriptografi. Sedemikian ketatnya regulasi ini sehingga eksportir pada bidang ini merasakan bahwa kebijakan pemerintahnya telah menempatkan mereka pada persaingan bisnis yang tidak menguntungkan bahkan sangat merugikan. Karena pada saat yang sama ternyata negara negara lain yang memiliki produk dan teknologi yang mirip malah tidak menerapkan kebijakan eksport apapun. Dengan demikian selalu ada kepentingan yang berbeda dan bertolak belakang antara dunia bisnis dengan sudut pandang keamanan nasional. Hal ini tentunya menjadi tantangan tersendiri bagi implementasi layanan kriptografi berbasis cloud khususnya dalam konsep CaaS (Cryptography as a Service).

KESIMPULAN

Ketersediaan layanan cloud untuk kriptografi adalah merupakan salah satu issue yang harus didalami. Salah satu kepentingannya adalah karakteristik layanan cloud yang bersifat *borderless* dan membutuhkan pendekatan yurisdiksi lintas negara. Hal ini mengingat teknologi kriptografi adalah termasuk dalam katagori ‘dual use”, yaitu sebuah teknologi yang harus diatur penggunaannya karena dapat digunakan untuk kepentingan komersil maupun kepentingan militer, sehingga apabila ternyata kedepannya teknologi ini dapat dengan mudah didapat dan ditawarkan melalui layanan cloud maka hampir mustahil untuk melakukan pengawasan terhadap penggunaan teknologi kriptografi di masyarakat nantinya. Hal ini tentunya juga berlaku pada salah model layanan kriptografi

berbasis cloud yaitu Cryptography as a Service (CaaS).

Berdasarkan uraian sebelumnya terihat bahwa issue utama CaaS adalah tentang *end point cryptography*, yaitu pada permasalahan tentang meletakkan kunci kriptografi pada *end point device* yang akan menimbulkan resiko tersendiri dan sangat rentan dengan vulnerabilitas. Pada issue ini *end point* device dipandang sebagai *bad place* untuk menghasilkan *key generator*. Solusinya adalah dengan menyiapkan provider untuk membantu *end point device* menjalankan operasi kriptografi melalui web services tanpa mengekspos kuncinya kepada *end point device* tersebut.

Solusi CaaS yang diberikan oleh [7], [9] sebenarnya memberikan harapan akan kemudahan dalam mengimplementasikan kebutuhan teknologi kriptografi yang diperlukan oleh berbagai aplikasi yang dijalankan diatas perangkat end point (misalnya handphone dan layanan e-givernment). Karena itu melalui studi ini walaupun masih terbatasnya kajian literature seputar CaaS namun telah didapat gambaran bagaimana sebenarnya model bisnis dan cara kerja CaaS tersebut. Beberapa hal masih harus dikaji lebih lanjut tentang issue CaaS antara lain adalah menyangkut masalah issue yurisdiksi penerapan kriptografi pada layanan cloud, penerapan HSM sebagai platform untuk mesin pada cryptography provider serta penggunaan TLS sebagai media komunikasi antara provider dengan end point device.

DAFTAR PUSTAKA

[1] N. Saper, “International Cryptography Regulation and the Global Information Economy,” *Northwest. J. Technol. Intellect. Prop.*, vol. 11, no. 7, 2013.

[2] M. Wang and L. Liu, “CRYPTO AS A SERVICE,” in *International Workshop on Cloud Computing and Information Security (CCIS)*, 2013.

[3] H. A. W. Ideler, “Cryptography as a service in a cloud computing environment,” Eindhoven University of Technology, 2012.

[4] S. Kumari, “Exploring Classical Security Techniques for Cloud Computing Environment,” *Int. J. Comput. Appl.*, vol. 4, no. 4, 2014.

[5] J. Hwang and H. Chuang, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service," *2011 Int. Conf. Inf. Sci. Appl.*, pp. 1–7, Apr. 2011.

[6] H. Rahmani, E. Sundararajan, Z. M. Ali, and A. M. Zin, "Encryption as a Service (EaaS) as a Solution for Cryptography in Cloud," *Procedia Technol.*, vol. 11, no. Iceei, pp. 1202–1210, 2013.

[7] P. Robinson, "Cryptography As A Service." RSA Europe Conference, 2013.

[8] V. Varadharajan and U. Tupakula, "Security as a Service Model for Cloud Environment," *IEEE Trans. Netw. Serv. Manag.*, vol. 11, no. 1, pp. 60–75, 2014.

[9] P. Robinson, "Applying Cryptography as a Service to Mobile Applications." 2014.

[10] Y. Prayudi and T. K. Priyambodo, "Study on Cryptography as a Service (CAAS)," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 10, pp. 150–156, 2014.

[11] S. Bleikertz, S. Bugiel, and H. Ideler, "Client-controlled Cryptography-as-a-Service in the Cloud," *Appl. Cryptogr. ...*, 2013.

[12] G. Hogben and M. Dekker, "The top ten information security risks for smartphone users.," 2010.

[13] R. Alshboul, "Security and Vulnerability in the E-Government Society," *Contemp. Eng. Sci.*, vol. 5, no. 5, pp. 215–226, 2012.

[14] G. R. Karokola, "A Framework for Securing e-Government Services The Case of Tanzania," Stockholm University, Sweden, 2012.

[15] S. Alshomrani and S. Qamar, "Cloud Based E-Government : Benefits and Challenges," *Int. J. Multidiscip. Sci. Eng.*, vol. 4, no. 6, pp. 15–19, 2013.

[16] S. Hashemi, K. Monfaredi, and M. Masdari, "Using Cloud Computing for E-Government : Challenges and Benefits," *Int. J. Comput. Information, Syst. Control Eng.*, vol. 7, no. 9, pp. 596–603, 2013.

[17] Smitha and Chitharanjan, "Security of Data in Cloud based E-Governance

System," *Spec. Issue Int. J. Comput. Appl.*, no. June, pp. 1–6, 2012.

[18] Y. Dodis, "The Cost of Cryptography," *Nautilus*, 2013. [Online]. Available: http://nautil.us/issue/7/waste/the-cost-of-cryptography.

[19] J. S. Sauver, "Cryptographic Best Practices in the Post-Snowden Era." Security Profesional 2014, St Louis Missouri, 2014.

[20] T. Field, "Cryptography in the Cloud," *Bank Info Security*, 2011. [Online]. Available: http://www.bankinfosecurity.com/cryptography-in-cloud-a-3305/op-1.

[21] J. B. Altman and W. Mcglone, "Demystifing U.S. Encryption Export Controls," *Am. Univ. Law Rev.*, vol. 46, no. 1975, pp. 493–510, 1987.