ANALISIS FAKTOR-FAKTOR YANG MEMPENGARUHI TINGKAT PENGGUNAAN SISTEM KEAMANAN EMAIL DI INDONESIA

Yanto
Program Studi Informatika, Universitas Indraprasta PGRI
otnay82@gmail.com

Abstrak

Sistem keamanan email memiliki peranan yang vital dalam menjaga keaslian dan kerahasiaan dari pesan yang dikirimkan. Akan tetapi sampai saat ini masih banyak individu maupun perusahaan yang belum menggunakannya, sehingga membuka peluang bagi serangan-serangan *cybercrime* yang melibatkan email. Penelitian ini bertujuan untuk mengetahui faktor-faktor yang menyebabkan rendahnya penggunaan fitur-fitur keamanan email, untuk kemudian memberikan sejumlah rekomendasi yang dapat diterapkan untuk meningkatkan penggunaan fitur-fitur tersebut. Penelitian ini dilakukan menggunakan metodologi *survey research*, dimana data-data yang digunakan untuk proses analisis dan pembahasan dikumpulkan melalui survei (menggunakan kuesioner) terhadap para pengguna email. Dari hasil penelitian diharapkan dapat meningkatkan penggunaan fitur-fitur keamanan email, meningkatkan kepercayaan terhadap keamanan komunikasi melalui email dan sebagai referensi bagi penelitian di masa yang akan datang. Berdasarkan hasil survei dan analisis, didapatkan kesimpulan faktor-faktor yang menyebabkan rendahnya tingkat penggunaan sistem keamanan email, diantaranya kurangnya dukungan fitur-fitur keamanan email, kurangnya sosialisasi fitur dan pengetahuan pengguna, *usability* serta beberapa program email belum mendukung fitur-fitur keamanan email. Dari faktor-faktor penghambat tersebut ada beberapa hal yang dapat dilakukan untuk mengatasinya, diantaranya sosialisasi fitur keamanan email, otomasi proses enkripsi/tanda tangan digital dan implementasi fitur enkripsi dan tanda tangan digital.
Kata kunci: Sistem keamanan email**,** enkripsi, tanda tangan digital

Abstract

The email security system has vital role in maintaining the authenticity and confidentiality of the messages sent. However, until now there are many individuals and companies who have not use it, those opening up opportunities for cybercrime attacks involving emails. This research aims to determine the factors that cause the low use of email security features, then provide number of recommendations that can be applied to increase the use of these features. This research was conducted using survey research methodology, where the data used for analysis and discussion are collected through surveys (using questionnaires) to email's user. The result of the research are expected to increase the use of email security features, increase trust in secure email communication and as reference for the future research. Based on the results of survey and analysis, the factors which cause low use of email security systems, including lack of support for email security features, lack of socialitation of the feature and user knowledge, and some email programs does not support the email security features. From these inhibiting factors, there are a number of things that can be done to overcome them, including socializing email security features, automating and implementing the encryption and digital signature features.
Keywords: *Email security system, encryption, digital signature*

1. PENDAHULUAN

Masih banyak individu atau perusahaan yang belum mengerti dan memahami akan pentingnya sistem keamanan pada email. Banyak terjadi kasus-kasus *cybercrime* yang dilakukan pada sistem email seperti pembobolan server email, pembocoran informasi rahasia yang dikirimkan melalui email serta tindak pemalsuan pesan atau identitas yang bertujuan untuk melakukan pencurian data pribadi (*phising*).

Penelitian ini bertujuan untuk mengetahui faktor-faktor yang menyebabkan rendahnya penggunaan fitur-fitur keamanan email pada saat ini, untuk kemudian memberikan sejumlah rekomendasi yang dapat diterapkan untuk meningkatkan penggunaan fitur-fitur tersebut.

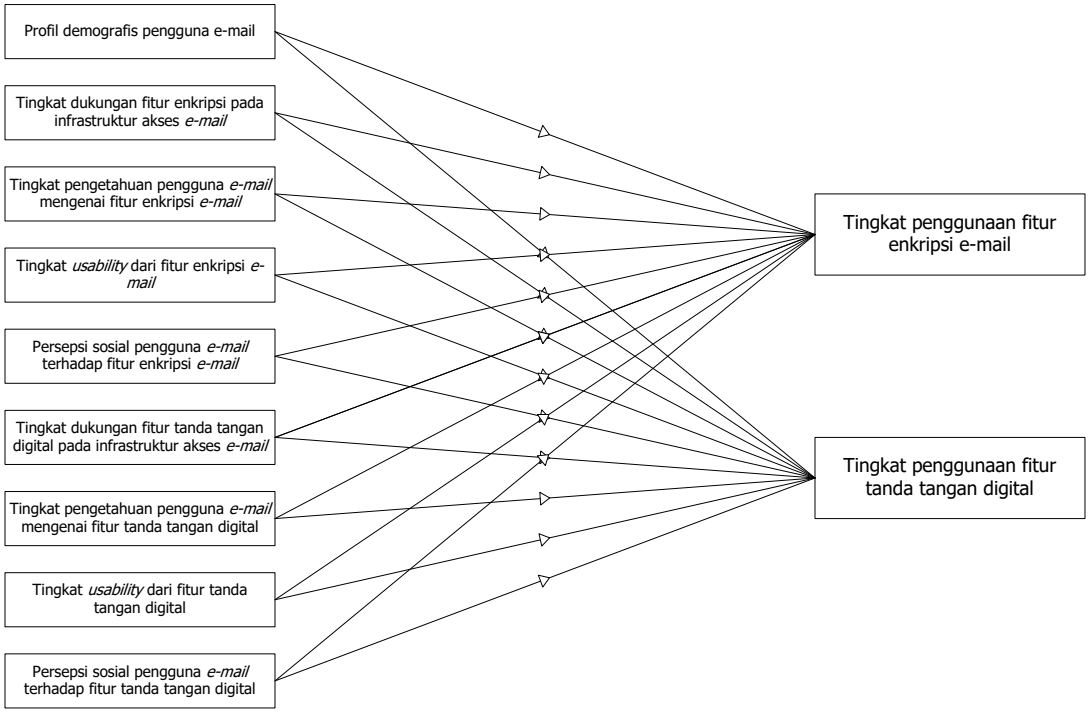
Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:
1) Meningkatkan penggunaan fitur-fitur keamanan yang terdapat pada sistem keamanan email, sehingga dapat membantu mencegah *potential loss* yang disebabkan oleh berbagai jenis gangguan keamanan (seperti bocornya informasi, perubahan isi pesan dan pencurian identitas) yang dapat terjadi pada sistem transmisi email.
2) Meningkatkan kepercayaan terhadap keamanan komunikasi lewat email, sehingga membantu mempercepat suksesnya gerakan *paperless office* pada perusahaan-perusahaan dalam rangka peningkatan efisiensi proses bisnis disamping juga menjaga kelestarian lingkungan hidup.
3) Sebagai referensi bagi penelitian/perancangan selanjutnya di masa yang akan datang, secara umum dalam bidang keamanan Teknologi Informasi dan secara khusus dalam analisa dan perancangan sistem keamanan email yang dapat digunakan secara efektif oleh para pengguna email.

Email adalah salah satu aplikasi yang paling populer pada internet, yang digunakan untuk melakukan komunikasi antar pengguna internet dengan cepat tanpa dibatasi oleh jarak dan waktu. Dengan naiknya tingkat penggunaan email (yang diikuti juga dengan ancaman keamanan pada jaringan internet) dengan sangat cepat, maka penerapan fitur keamanan pada sistem email (khususnya yang berkaitan dengan keaslian dan kerahasiaan pesan yang dikirimkan) menjadi suatu hal yang penting.

Pada saat ini sebagian besar sistem webmail publik yang populer seperti Hotmail, Yahoo! Mail dan Gmail telah menerapkan fitur-fitur keamanan yang cukup *usable* dalam menangkal serangan *cybercrime* melalui email seperti *phishing*, *hacking* dan virus/worm [1]; walaupun belum lengkap (karena secara *default* belum memiliki fitur untuk enkripsi email).

Berbeda dengan sistem webmail publik, sejumlah program email (seperti Microsoft Outlook dan Mozilla Thunderbird) telah memiliki dukungan fitur keamanan email secara *built-in* melalui implementasi standar S/MIME. S/MIME ini merupakan standar *de facto* bagi penerapan fitur enkripsi maupun tanda tangan digital pada pesan-pesan email berbasis MIME yang dilakukan melalui penggunaan sertifikat kunci publik dari *Certificate Authority*, dengan mekanisme kerja yang serupa dengan PGP [2].

Dalam penelitian ini, variabel-variabel yang akan diteliti meliputi sebelah variabel yang terdiri dari sembilan variabel bebas (*independent variable*) dan dua variabel terikat (*dependent variable*).



Gambar 1. *Framework* Penelitian

Terdapat dua macam hipotesis yang perlu digunakan pada penelitian, yaitu [3]:

1) Hipotesis nol (Ho)

Hipotesis ini dinamakan hipotesis nol karena memiliki bentuk dasar pernyataan yang menyatakan bahwa tidak ada (nol) hubungan antara variabel bebas dan variabel terikat. Pada umumnya hipotesis nol ini dibuat untuk kemungkinan besar ditolak.

a. **Ho1**: Profil demografis pengguna email tidak berpengaruh terhadap penggunaan fitur enkripsi email.

b. **Ho2**: Tingkat dukungan fitur enkripsi pada infrastruktur akses email tidak berpengaruh terhadap penggunaan fitur enkripsi email.

c. **Ho3**: Tingkat pengetahuan pengguna email mengenai fitur enkripsi email tidak berpengaruh terhadap penggunaan fitur enkripsi email.

d. **Ho4**: Tingkat *usability* dari fitur enkripsi email tidak berpengaruh terhadap penggunaan fitur enkripsi email**.**

e. **Ho5**: Persepsi sosial pengguna email terhadap fitur enkripsi email tidak berpengaruh terhadap penggunaan fitur enkripsi email.

f. **Ho6**: Profil demografis pengguna email tidak berpengaruh terhadap penggunaan fitur tanda tangan digital.

g. **Ho7**: Tingkat dukungan fitur tanda tangan digital pada infrastruktur akses email tidak berpengaruh terhadap penggunaan fitur tanda tangan digital.

h. **Ho8**: Tingkat pengetahuan pengguna email mengenai fitur tanda tangan digital tidak berpengaruh terhadap penggunaan fitur tanda tangan digital.

i. **Ho9**: Tingkat *usability* dari fitur tanda tangan digital tidak berpengaruh terhadap penggunaan fitur tanda tangan digital.

j. **Ho10**: Persepsi sosial pengguna email terhadap fitur tanda tangan digital tidak berpengaruh terhadap penggunaan fitur tanda tangan digital.

2) Hipotesis Alternatif (Ha)

Hipotesis alternatif merupakan hipotesis yang berlawanan dengan

hipotesis nol, dimana hipotesis ini menyatakan ada hubungan antara variabel bebas dan variabel terikat. Hipotesis alternatif dapat langsung dirumuskan apabila pada suatu penelitian hipotesis nol ditolak.

a. **Ha1**: Profil demografis pengguna email berpengaruh terhadap penggunaan fitur enkripsi email.
b. **Ha2**: Tingkat dukungan fitur enkripsi pada infrastruktur akses email berpengaruh terhadap penggunaan fitur enkripsi email.
c. **Ha3**: Tingkat pengetahuan pengguna email mengenai fitur enkripsi email berpengaruh terhadap penggunaan fitur enkripsi email.
d. **Ha4**: Tingkat *usability* dari fitur enkripsi email berpengaruh terhadap penggunaan fitur enkripsi email.
e. **Ha5**: Persepsi sosial pengguna email terhadap fitur enkripsi email berpengaruh terhadap penggunaan fitur enkripsi email.
f. **Ha6**: Profil demografis pengguna email berpengaruh terhadap penggunaan fitur tanda tangan digital.
g. **Ha7**: Tingkat dukungan fitur tanda tangan digital pada infrastruktur akses email berpengaruh terhadap penggunaan fitur tanda tangan digital.
h. **Ha8**: Tingkat pengetahuan pengguna email mengenai fitur tanda tangan digital berpengaruh terhadap penggunaan fitur tanda tangan digital.
i. **Ha9**: Tingkat *usability* dari fitur tanda tangan digital berpengaruh terhadap penggunaan fitur tanda tangan digital.
j. **Ha10**: Persepsi sosial pengguna *email* terhadap fitur tanda tangan digital berpengaruh terhadap penggunaan fitur tanda tangan digital.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan *survey research* yang dilakukan secara eksploratif, dimana peneliti melakukan survey untuk menyelidiki tentang penggunaan sistem keamanan email di masyarakat, dalam rangka menginvestigasi mengenai faktor-faktor apa saja yang mempengaruhi tingkat penggunaan sistem keamanan email serta seberapa besar pengaruh dari faktor-faktor tersebut terhadap penggunaan sistem keamanan email di lapangan.

Agar proses survey yang dilakukan terarah, maka perlu ditentukan secara jelas populasi dan sampel yang digunakan untuk proses pelaksanaan survey. Populasi yang akan diteliti adalah para mahasiswa, komunitas professional TI dan komunitas pengguna TI secara umum di Indonesia yang telah terbiasa dengan penggunaan email untuk pekerjaan sehari-hari.

Dengan berlandaskan pada variabel dan hipotesis penelitian, maka disusunlah kuesioner untuk mengumpulkan data mengenai profil pengguna email beserta tingkat pengetahuan, *usability* dan penggunaan dari fitur-fitur keamanan email yang dibahas. Dalam hal ini pertanyaan-pertanyaan yang diajukan akan mengacu antara lain pada pertanyaan-pertanyaan survey yang terdapat pada [4], kesulitan-kesulitan yang dialami oleh pengguna sistem keamanan email [4], [5] serta aplikasi-aplikasi email (dalam bidang *e-commerce* dan lainnya) yang membutuhkan keamanan khusus disamping juga profil demografis dan pola penggunaan email dari para responden.

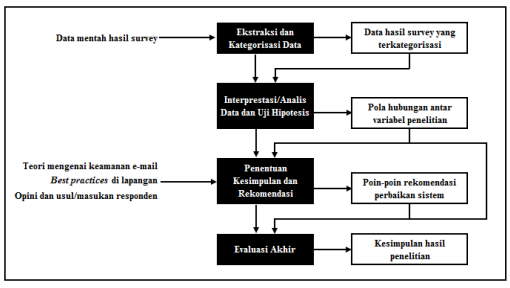
Kuesioner ini merupakan kuesioner tahap awal/*pretest*, yang berarti setelah penyusunan kuesioner akan dilakukan pengujian awal/*pretest* dan perbaikan untuk meningkatkan kualitas kuesioner. Proses *pretest* dilakukan untuk mengetahui kekurangan-kekurangan dari desain kuesioner, yang mencakup hal-hal berikut [6]:

a. Apakah pertanyaan-pertanyaan pada kuesioner dapat dimengerti dengan baik?
b. Apakah terdapat pertanyaan yang perlu diubah?
c. Apakah urutan pertanyaan perlu diubah?
d. Apakah ada pertanyaan yang dirasa sensitif atau tabu?

Dari hasil *pretest* didapatkan bahwa masih banyak perbaikan yang perlu dilakukan. Kuesioner yang telah disempurnakan dipandang siap untuk disebarkan kepada seluruh sampel responden yang dipilih untuk proses pengumpulan data.

Penelitian ini menggunakan instrumen kuesioner yang didalamnya terdapat sejumlah pernyataan tertulis yang digunakan untuk memperoleh tanggapan dan informasi dari responden. Selain itu diperlukan perangkat keras dan perangkat lunak yang digunakan untuk menganalisa data hasil survey.

Proses analisis data hasil survey dilakukan setelah proses survey kuesioner selesai dilakukan, proses analisis ini dapat diuraikan lagi menjadi sejumlah proses sebagai berikut:



Gambar 2. Alur Tahap Analisis Data

1) Ekstraksi dan Kategorisasi Data

Pada proses ini data hasil survey yang telah diperoleh melalui kuesioner diekstrak ke dalam bentuk yang dapat diolah secara statistik, untuk kemudian dilakukan kategorisasi dalam rangka persiapan untuk proses analisis dan interpretasi data.

2) Interprestasi/Analisa Data dan Uji Hipotesis

Setelah data hasil survey diekstraksi dan dikategorisasi, pada proses ini dilakukan interpretasi dan analisis data dalam rangka mengetahui pola hubungan antar variabel dan menguji hipotesis-hipotesis penelitian yang telah ditetapkan.

3) Penetuan Kesimpulan dan Rekomendasi

Dalam tahap ini dengan menarik kesimpulan dari hasil interpretasi data dan pengujian hipotesis, akan disusun poin-poin rekomendasi yang dapat diterapkan untuk mencapai tujuan penelitian.

4) Evaluasi Akhir

Berdasarkan hasil evaluasi mengenai faktor-faktor yang mempengaruhi tingkat penggunaan sistem keamanan email dan poin-poin rekomendasi yang dibuat, akan ditarik kesimpulan hasil penelitian.

3. HASIL DAN PEMBAHASAN

Penyebaran dan pengumpulan kuesioner pada penelitian ini dilakukan secara *on-line* dan *off-line* dan didapatkan total 138 responden, dimana 105 responden melakukan pengisian terhadap minimal satu pertanyaan yang terdapat pada kuesioner dan 53 diantaranya mengisi seluruh pertanyaan pada kuesioner dengan lengkap (untuk menghindari kesan pemaksaan terhadap responden serta untuk menjaga *privacy* mereka, semua pertanyaan pada survey bersifat *optional*).

Karena pertanyaan-pertanyaan pada kuesioner tidak seluruhnya bersifat *critical* dan jumlah responden yang dirasakan tidak terlalu banyak, maka diputuskan bahwa analisis yang dilakukan akan melibatkan juga hasil survey responden yang tidak lengkap (akan tetapi untuk menghindari bias sistemik, dalam analisis hubungan

antar variabel hanya akan dimasukkan data-data yang tidak memiliki nilai *blank* pada pasangan variabel yang diuji).

Untuk menghindari bias, pada survey ini setiap orang responden dibatasi hanya dapat melakukan pengisian kuesioner sebanyak satu kali akan tetapi responden tersebut dapat kembali untuk merevisi/menambah jawabannya apabila diinginkan. Secara keseluruhan proses pengisian dan pengumpulan kuesioner ini dilakukan dalam jangka waktu yang cukup panjang, hal ini dilakukan dalam rangka menghimpun lebih banyak responden (dalam hal ini agar hasil survey memiliki akurasi yang cukup baik, jumlah responden ditargetkan minimal 100 orang). Setelah berhasil dikumpulkan cukup banyak responden yang menjawab kuesioner, maka survey ditutup untuk kemudian dilakukan proses analisis data.

Selanjutnya data hasil survey diekstrak ke dalam format Microsoft Excel, untuk kemudian dilakukan kategorisasi data dalam rangka persiapan untuk proses analisis/interpretasi data. Proses kategorisasi data ini dilakukan berdasarkan variabel-variabel yang tercakup dalam hipotesis penelitian, antara lain faktor demografis responden (jenis kelamin, usia, pendidikan, pekerjaan), penggunaan email oleh responden (lama penggunaan dalam tahun, platform dan program yang digunakan, lokasi akses email) serta tingkat pengetahuan dan penggunaan dari para responden terhadap fitur-fitur enkripsi dan tanda tangan digital.

Setelah dilakukan ekstraksi dan kategorisasi data, maka didapatkan satu set data responden yang siap untuk dianalisis. Sebelum melangkah ke tahap analisis, pembahasan hasil survey berikut ini akan memaparkan hasil survey yang diperoleh dalam bentuk narasi.

1) **Profil Demografis Responden**

Usia rata-rata responden adalah 27 tahun, dimana 76% adalah pria dan 24% adalah wanita. Rata-rata responden memiliki tingkat pendidikan yang cukup baik, dengan mayoritas (70%) berpendidikan S1 dan sisanya berpendidikan S2 (12%), Diploma (4%), SMU (13%) dan SD (1%). Para responden memiliki pekerjaan yang cukup beragam dimana sebagian besar diantaranya (67%) mengaku bekerja sebagai pegawai swasta, jawaban-jawaban lain dari para responden antara lain pegawai negeri sebanyak 4%, wiraswasta 11%, belum bekerja 18%, mahasiswa/pelajar 5%, instruktur/dosen 3% dan pensiunan 1%.

2) **Pola Penggunaan Email**

Para responden memperoleh email *account* mereka untuk pertama kalinya antara tahun 1992-2006, dengan lebih dari separuhnya (55%) mulai menggunakan email antara tahun 1998-2000 pada saat *dot-com booming.* Seluruh responden mengakses email melalui *platform* Microsoft Windows, dua *platform* lain adalah *platform* Unix/Linux (15,62%) dan *platform mobile* (27,08%). Para responden menggunakan berbagai jenis program email untuk mengakses email, pilihan utama program akses email adalah *webmail* (dipilih oleh 91% responden, dengan 25% diantaranya menggunakan *webmail* sebagai satu-satunya sarana akses email) yang disusul oleh Microsoft Express (51%), Outlook Express (39%) dan Mozilla Mail (27%) dan aplikasi *mobile* (22%).

Sebagian besar pengguna email melakukan akses email mereka melalui berbagai lokasi berbeda termasuk lokasi-lokasi akses *shared*/publik (72% responden mengakses email mereka

dari komputer kantor, 53% dari warung Internet, dan 40% dari perpustakaan/lab).

3) **Pengetahuan Pengguna Email Mengenai Fitur Enkripsi**

Sebanyak 46% responden menyatakan bahwa mereka sudah pernah menerima email terenkripsi dan 34% lainnya menyatakan belum, sementara sisanya (20%) menyatakan tidak tahu. Bentuk-bentuk enkripsi yang dilaporkan oleh para responden yang sudah pernah menerima email terenkripsi beragam, dengan jenis-jenis enkripsi yang umum dilaporkan mencakup antara lain SSL pada *webmail* (oleh 48% responden yang pernah menerima email terenkripsi), *attachment* pesan yang dilindungi oleh *password* (55%), *trusted signature* (32%), pesan yang dienkripsi dengan PGP/S-MIME (28%), dan tidak tahu (sebanyak 15%).

4) ***Awareness* mengenai Dukungan Fitur Enkripsi pada Program Email**

Berkenaan dengan *support* penggunaan fitur enkripsi pada program email, 48% responden menyatakan bahwa program email yang mereka gunakan mendukung fitur enkripsi, 7% menyatakan tidak mendukung dan sisanya 45% menyatakan tidak tahu.

5) **Manajemen Penyimpanan Kunci Privat**

Resiko enkripsi sudah diketahui dan disadari oleh cukup banyak responden, dimana 56% responden menyatakan telah mengetahui fakta tersebut, sebanyak 45% dari responden ingin mengelola penyimpanan email terenkripsi dan/atau kunci digitalnya secara manual dan 37% responden lain memilih menyerahkan pengelolaan penyimpanan email terenkripsi dan kunci privat kepada komputer/mesin/pihak ketiga, sedangkan 18% responden sisanya masih ragu-ragu mengenai metode pengelolaan yang tepat.

Dengan munculnya masalah-masalah kerahasiaan kunci yang ditimbulkan di satu sisi (keterbukaan akses kunci privat bagi pemerintah apabila dibutuhkan, serta kemungkinan serangan oleh "orang dalam" dan *hacker* terhadap kunci yang disimpan [6]) dan kepastian akses berkelanjutan pada kunci privat di sisi lain (selama *key escrow* masih bekerja), hal ini menimbulkan beragam reaksi dari para responden yang disurvey. Dalam hal ini terdapat sedikit kecenderungan kurang setuju dengan penggunaan *key escrow*, seperti yang diperlihatkan pada diagram hasil survey (sangat setuju 8% dan setuju 27% versus tidak setuju 24% dan sangat tidak setuju 21%).

6) **Kebutuhan Penggunaan Fitur Enkripsi Email**

Fitur enkripsi email digunakan untuk mengamankan isi pesan email yang bersifat sensitif/rahasia dari orang-orang yang tidak berhak, sudah semestinya email yang berisi informasi-informasi finansial seperti surat dari bank/kartu kredit, bukti transaksi *e-commerce*, dan tagihan pajak dilindungi dengan enkripsi; hal ini didukung oleh hasil survey dimana 94%, 82% dan 55% responden setuju bahwa enkripsi dibutuhkan untuk masing-masing jenis email tersebut. Prioritas selanjutnya untuk enkripsi adalah email komunikasi pribadi, dimana enkripsi untuk komunikasi pada lingkungan kantor (50%) dianggap lebih penting daripada untuk komunikasi pada lingkungan rumah (27%), dikarenakan sejumlah faktor seperti penggunaan bersama komputer dan hal-hal "rahasia perusahaan" yang mungkin dibahas pada komunikasi antar rekan sekantor.

7) **Tingkat Pemahaman Mengenai Enkripsi**

Secara subyektif para responden menyatakan tingkat pemahaman mengenai enkripsi yang beragam (mulai dari tidak tahu sama sekali sampai dengan sangat baik), dengan sedikit kecenderungan pemahaman yang kurang baik (pada skala *likert* dari 1 sampai dengan 5 dimana 1 = sangat baik dan 5 = tidak tahu sama sekali; didapat parameter statistik n = 85 orang; μ = 3,071 dan σ = 1,1).

8) **Kendala Yang Dihadapi Pada Pengiriman Email Terenkripsi**

Dari 82 responden yang mengisi bagian ini, sebagian besar menjawab bahwa mereka jarang (30 orang = 37%) atau tidak pernah (33 orang = 40%) mengirimkan email terenkripsi, total hanya 16% responden yang menjawab "selalu" atau "kadang-kadang".

Dari pertanyaan selanjutnya mengenai alasan tidak melakukan enkripsi email, nampak bahwa sebagian besar responden (59 orang = 84% dari responden yang menjawab "jarang"/"tidak pernah" atau 72% dari keseluruhan responden yang mengisi bagian survey ini) tidak menggunakan fitur enkripsi karena merasa fitur ini tidak dibutuhkan. Sedangkan alasan-alasan lain yang dikemukakan antara lain tidak begitu peduli dengan keamanan yang diberikan oleh enkripsi (13% dari responden yang mengisi bagian ini), terlalu sulit/repot untuk digunakan (18%), tidak tahu caranya (28%), dan khawatir penerima tidak dapat membaca email terenkripsi yang dikirimkan (46%).

9) **Kesulitan Saat Melakukan Enkripsi Email**

Kesulitan utama adalah ketidaktahuan akan cara melakukan enkripsi email (oleh 32% responden). Kesulitan-kesulitan lain yang dihadapi antara lain ketidaktahuan mengenai kunci mana yang tepat untuk melakukan enkripsi email (15%), lupa *passphrase* yang digunakan (17%), tidak yakin apakah enkripsi berhasil dilakukan (22%), tidak tahu jenis kesulitan yang dihadapi (12%), dan khawatir penerima pesan tidak dapat membaca pesan terenkripsi yang dikirimkan (1%).

10) **Kesulitan Saat Melakukan Dekripsi Email**

Hasil survey menunjukkan hal yang hampir sama (33% responden tidak tahu langkah-langkah dekripsi, 22% tidak tahu kunci dekripsi yang tepat, 27% lupa *passphrase*, 10% kesulitan melihat hasil dekripsi dan 12% lainnya tidak tahu mengenai jenis kesulitan yang dihadapinya). Bahkan menurut hasil survey proses dekripsi ini lebih 'sulit' dari enkripsi, karena lebih sedikitnya jumlah responden yang menyatakan bahwa mereka tidak menemukan kesulitan berarti (21% pada dekripsi versus 29% pada enkripsi).

11) **Kesulitan Terkait Manajemen Kunci Publik/Privat**

Hasil survey menunjukkan beragam jenis kesulitan yang dihadapi oleh sejumlah besar responden dalam menggunakan sistem manajemen kunci ini; yang dimulai dari tidak tahu cara membuat pasangan kunci (27%), tidak tahu cara mempublikasikan kunci publik yang sudah dibuat (19%), tidak dapat membedakan kunci publik dan privat (22%), sulit memperoleh kunci publik orang lain (27%), dan kurang percaya akan keaslian kunci publik yang diperoleh dari orang lain (21%); hanya 23% dari responden yang menyatakan bahwa mereka tidak memperoleh kesulitan berarti.

12) **Penerimaan Email dengan Tanda Tangan Digital**

Sebanyak 45% responden menyatakan bahwa mereka sudah pernah menerima

email yang ditandatangani secara digital, 41% lainnya menyatakan belum pernah sedangkan sisanya (14%) menyatakan tidak tahu.

13) **Konsep Enkripsi dan Tanda Tangan Digital**

Lebih dari separuh (58%) responden mengetahui bahwa terdapat perbedaan antara fitur enkripsi dengan tanda tangan digital. Di sisi lain 7% responden menganggap bahwa kedua fitur itu sama, sedangkan 35% responden sisanya menyatakan tidak tahu.

Sedangkan mengenai kegunaan tanda tangan digital dalam verifikasi identitas pengirim email terenkripsi, fakta ini diketahui oleh hanya 51% dari responden sedangkan 14% responden menganggapnya tanda tangan tersebut tidak berguna, 35% sisanya menyatakan tidak tahu fakta ini semakin menegaskan adanya kekaburan/*blurness* antara konsep kegunaan dari kedua fitur keamanan email tersebut.

14) **Metafora Bentuk dan Analogi Tanda Tangan Digital**

Dari bentuk-bentuk tanda tangan digital yang ada, 30% responden cenderung menginginkan tanda tangan digital ditempatkan sebagai sebaris teks pada *header* pesan, 50% sebagai lambang pita/sertifikat di *inbox* dan 59% sebagai tanda tangan pada akhir pesan (seperti pada tanda tangan konvensional).

Mengenai analogi yang cocok bagi tanda tangan digital, sebanyak 55% responden menganggap tanda tangan digital sebagai analogi dari tanda tangan "biasa" yang dibuat dengan tinta, 45% menganalogikan dengan pengesahan/notarisasi pesan dan 28% dengan sidik jari. Dalam hal ini keberagaman metafora dan analogi yang dipilih merefleksikan sifat teknologi tanda tangan digital saat ini yang bersifat ambigu, karena memiliki dua sisi: pelindung integritas isi pesan (seperti segel) dan identifikasi pengirim pesan [7] (seperti tanda tangan konvensional).

15) **Kebutuhan Penggunaan Fitur Tanda Tangan Digital**

Seperti pada enkripsi, prioritas utama bagi penandatanganan digital ini adalah email yang berisi informasi-informasi finansial seperti surat dari bank/kartu kredit, bukti transaksi *e-commerce*, dan tagihan pajak. Hal ini didukung oleh hasil survey yang menunjukkan bahwa 95%, 89% dan 55% responden setuju bahwa tanda tangan digital dibutuhkan untuk masing-masing jenis email tersebut. Dan (sama seperti enkripsi) prioritas selanjutnya jatuh pada email komunikasi pribadi, dimana tanda tangan digital lebih penting untuk komunikasi pada lingkungan kantor (31%) dibandingkan komunikasi pada lingkungan rumah (12%) mengingat faktor-faktor potensi gangguan keamanan dan/atau pemalsuan pesan yang lebih besar disana.

16) **Tingkat Pemahaman Mengenai Tanda Tangan Digital**

Tingkat pemahaman para responden mengenai tanda tangan digital (yang diukur secara subyektif melalui pertanyaan survey) sangat beragam, dengan kecenderungan pemahaman yang kurang baik (sangat baik 6% dan baik 17% versus kurang 31% dan tidak tahu sama sekali 8%).

17) **Pengiriman Email dengan Tanda Tangan Digital**

Dari 62 responden yang mengisi bagian ini, sebagian besar menjawab bahwa mereka jarang (16 orang = 26%) atau tidak pernah (36 orang = 58%) mengirimkan email yang ditandatangani secara digital, dengan hanya 6 orang (10%) yang menjawab "selalu" atau "kadang-kadang". Alasan utama para responden untuk tidak

menggunakan tanda tangan digital adalah karena mereka merasa bahwa tanda tangan digital tidak dibutuhkan untuk aplikasi yang mereka gunakan (69%). Selain itu alasan-alasan lain yang dikemukakan antara lain tidak begitu peduli dengan keamanan yang diberikan oleh tanda tangan digital (21%), terlalu sulit/repot untuk digunakan (10%), dan tidak tahu cara membuatnya (27%).

18) **Kesulitan Terkait Tanda Tangan Digital**

Kesulitan-kesulitan yang dihadapi oleh para responden terkait dengan tanda tangan digital antara lain tidak tahu cara membuat (22%) dan memverifikasi (24%) tanda tangan digital, tidak tahu bentuk tanda tangan digital yang benar (17%), dan kurang percaya dengan keaslian tanda tangan digital yang diperoleh (17%).

19) **Kesediaan Mengganti/Meng-*upgrade* Program Email**

Dari seluruh responden, sebanyak 54% bersedia untuk mengganti/meng-*upgrade* program email yang mereka gunakan sedangkan 31% lainnya menyatakan tidak bersedia. Alasan-alasan yang dikemukakan oleh para responden yang tidak bersedia *upgrade* antara lain bahwa keamanan yang disediakan oleh program email yang digunakan sudah cukup baik (46%), hanya menggunakan *webmail* (46%), malas mengganti/meng-*upgrade* sistem yang digunakan (25%) dan sistem keamanan yang ada belum diperlukan/sesuai kebutuhan (8%).

Setelah keseluruhan hasil survey yang ada dipaparkan dan dianalisis, selanjutnya perlu dilakukan interpretasi dari hasil survey tersebut untuk mengetahui secara pasti hubungan antara variabel-variabel penelitian, dalam rangka menjawab pertanyaan penelitian mengenai faktor-faktor yang mempengaruhi tingkat penggunaan sistem keamanan email. Tabel berikut memberikan interprestasi hasil survey secara singkat dalam bentuk penerimaan/penolakan hipotesis-hipotesis penelitian serta alasannya.

Tabel 1. Interprestasi Hasil Survey dan Pengujian Hipotesis

Hipotesis Nol	Deskripsi	Terima Hipotesis Nol?
Ho1	**Bunyi hipotesis**: Profil demografis pengguna email tidak berpengaruh terhadap penggunaan fitur enkripsi email. **Fakta**: Tidak ditemukan hubungan statistikal yang signifikan pada taraf *confidence level* $\alpha \leq 0{,}05$ antara faktor-faktor demografis (jenis kelamin, umur, pendidikan dan pekerjaan) terhadap tingkat penggunaan fitur enkripsi email.	Terima
Ho2	**Bunyi hipotesis**: Tingkat dukungan fitur enkripsi pada infrastruktur akses email tidak berpengaruh terhadap penggunaan fitur enkripsi email. **Fakta**: • Ditemukan hubungan statistikal yang signifikan antara dukungan fitur enkripsi pada program email yang digunakan dengan tingkat penggunaan fitur enkripsi email. • Tidak ada diantara para pengguna webmail murni (yang tidak menggunakan program lain untuk mengakses email) yang mengetahui apalagi menggunakan enkripsi email berbasis PGP/S-MIME.	Tolak
Ho3	**Bunyi hipotesis**: Tingkat pengetahuan pengguna email mengenai fitur enkripsi email tidak berpengaruh terhadap penggunaan fitur enkripsi email. **Fakta**: • Terdapat korelasi yang cukup kuat antara variabel subyektif mengenai pengetahuan enkripsi dengan poin-poin pengetahuan enkripsi pada *checklist* pertanyaan survey → variabel subyektif ini valid. • Terdapat hubungan statistikal yang signifikan antara variabel subyektif mengenai pengetahuan enkripsi dengan tingkat penggunaan fitur enkripsi email. • Sehingga dapat disimpulkan	Tolak

	bahwa terdapat hubungan statistikal yang signifikan antara tingkat pengetahuan pengguna email mengenai fitur enkripsi dengan tingkat penggunaan fitur enkripsi email.	
Ho4	**Bunyi hipotesis**: Tingkat *usability* dari fitur enkripsi email tidak berpengaruh terhadap penggunaan fitur enkripsi email. **Fakta**: 63% responden mengalami masalah-masalah *usability* pada fitur enkripsi email yang menyebabkan mereka jarang/tidak pernah menggunakan fitur enkripsi email.	Tolak
Ho5	**Bunyi hipotesis**: Persepsi sosial pengguna email terhadap fitur enkripsi email tidak berpengaruh terhadap penggunaan fitur enkripsi email. **Fakta**: 72% responden mengaku jarang/tidak pernah menggunakan fitur enkripsi email karena merasa enkripsi email tidak dibutuhkan dalam konteks aktivitas mereka sehari-hari (faktor persepsi sosial).	Tolak
Ho6	**Bunyi hipotesis**: Profil demografis pengguna email tidak berpengaruh terhadap penggunaan fitur tanda tangan digital. **Fakta**: Tidak ditemukan hubungan statistikal yang signifikan pada taraf *confidence level* $\alpha \leq 0{,}05$ antara faktor-faktor demografis (jenis kelamin, umur, pendidikan dan pekerjaan) terhadap tingkat penggunaan fitur tanda tangan digital.	Terima
Ho7	**Bunyi hipotesis**: Tingkat dukungan fitur tanda tangan digital pada infrastruktur akses email tidak berpengaruh terhadap penggunaan fitur tanda tangan digital. **Fakta**: Ditemukan hubungan statistikal yang signifikan antara dukungan fitur tanda tangan digital pada program email yang digunakan dengan tingkat penggunaan fitur tanda tangan digital.	Tolak
Ho8	**Bunyi hipotesis**: Tingkat pengetahuan pengguna email mengenai fitur tanda tangan digital tidak berpengaruh terhadap penggunaan fitur tanda tangan digital. **Fakta**: • Terdapat korelasi yang cukup kuat antara variabel subyektif mengenai pengetahuan tanda tangan digital dengan poin-poin pengetahuan tanda tangan digital pada *checklist* pertanyaan survey → variabel subyektif ini valid. • Terdapat hubungan statistikal yang signifikan antara variabel subyektif mengenai pengetahuan tanda tangan digital dengan tingkat penggunaan fitur tanda tangan digital. • Sehingga dapat disimpulkan bahwa terdapat hubungan statistikal yang signifikan antara tingkat pengetahuan pengguna email mengenai fitur tanda tangan digital dengan tingkat penggunaan fitur tanda tangan digital.	Tolak
Ho9	**Bunyi hipotesis**: Tingkat *usability* dari fitur tanda tangan digital tidak berpengaruh terhadap penggunaan fitur tanda tangan digital. **Fakta**: Hanya 28% responden yang tidak mengalami masalah-masalah *usability* pada fitur tanda tangan digital, sementara terdapat 32% responden yang mengalami masalah *usability* yang cukup serius sehingga menyebabkan mereka jarang/tidak pernah menggunakan fitur tanda tangan digital.	Tolak
Ho10	**Bunyi hipotesis**: Persepsi sosial pengguna email terhadap fitur tanda tangan digital tidak berpengaruh terhadap penggunaan fitur tanda tangan digital. **Fakta**: 74% responden mengaku jarang/tidak pernah menggunakan fitur tanda tangan digital karena merasa tanda tangan digital tidak dibutuhkan dan/atau tidak meningkatkan keamanan sistem dalam konteks aktivitas mereka sehari-hari (persepsi sosial).	Tolak

Dari interpretasi hasil survey ditemukan 4 pasang faktor yang berpengaruh terhadap rendahnya penggunaan fitur-fitur keamanan email (dalam hal ini enkripsi dan tanda tangan digital) yaitu:

1) Dukungan fitur enkripsi dan tanda tangan digital pada infrastruktur akses email [8].
2) Pengetahuan pengguna email mengenai fitur enkripsi dan tanda tangan digital [4].
3) *Usability* dari fitur enkripsi dan tanda tangan digital [4],[9].

4) Persepsi sosial pengguna terhadap fitur enkripsi dan tanda tangan digital [10].

4. SIMPULAN

Berdasarkan hasil survey dan analisa pada bab-bab sebelumnya serta mengacu pada *research question*, maka kesimpulan yang didapat dari penelitian ini adalah:

1. Faktor-faktor yang menyebabkan rendahnya tingkat penggunaan sistem keamanan email di Indonesia:

a) Kurangnya dukungan fitur enkripsi email pada program email yang digunakan
b) Kurangnya pengetahuan pengguna email mengenai fitur enkripsi dan tanda tangan digital
c) *Usability* yang kurang baik
d) Sebagian besar pengguna email masih menganggap enkripsi dan tanda tangan digital belum dibutuhkan untuk keperluan sehari-hari

2. Hal-hal yang dapat dilakukan untuk mengatasi faktor-faktor penghambat diatas:

a) Terkait dengan fitur enkripsi email;
   - Sosialisasi fitur enkripsi email
   - Implementasi fitur enkripsi pada webmail
   - Otomasi proses enkripsi/dekripsi email
   - Otomasi manajemen kunci digital
b) Terkait dengan fitur tanda tangan digital;
   - Sosialisasi fitur tanda tangan digital
   - Penerapan standar baku tanda tangan digital
   - Otomasi proses pembuatan dan verifikasi tanda tangan digital

DAFTAR PUSTAKA

[1] Delany, Mark. *Domain-based Email Authentication Using Public-Keys Advertised in the DNS (DomainKeys)*. Yahoo! Inc., 2005.

[2] Garfinkel, Simson L. dan Miller, Robert C. *Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express*. SOUPS 2005, Pittsburgh, Pennsylvania, USA.

[3] Bungin, Burhan H.M. *Metodologi Penelitian Kuantitatif*. Edisi Kedua, Prenada Media Group, Jakarta, 2006.

[4] Garfinkel, Simson L. *et. al. How to Make Secure Email Easier To Use*. MIT CSAIL, 2005.

[5] Whitten, Alma dan Tygar, J. D. "Why Johnny can't encrypt: A usability evaluation of PGP 5.0". *USENIX Security Symposium*, 8 (1999), 169-184

[6] Singarimbun, M. dan Sofian, E. *Metode Penelitian Survai*. LP3ES, Jakarta, 1989.

[7] Garfinkel, Simson L.*Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable*. Thesis for Doctor of Philosophy (Ph.D), Department of Electrical Engineering and Computer Science, Massachusets Institute of Technology, 2005.

[8] Stallings, William. *Cryptography and Network Security: Principles and Practices*. *4th Edition*. Pearson International Edition, 2006.

[9] Abelson, Hal *et. al. The Risks of "Key Recovery", "Key Escrow", And "Trusted Third Party" Encryption*. A Report by an Ad Hoc Group of Cryptographers and Computer Scientists, Center for Democracy & Technology, 1998.

[10] Gaw, S., Felten, E.W. & Fernandez-Kelly, P. *Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted Email*. CHI 2006, Montreal, Quebec, Canada.