Skema Berbagi Informasi Keamanan Siber Menggunakan Model *Hub and Spoke* untuk Mendapatkan Kepercayaan dalam *Public-Private Partnership*

Farouq Aferudin
Badan Siber dan Sandi Negara, farouq.aferudin@bssn.go.id

Abstrak

Berbagi informasi keamanan siber menjadi salah satu bentuk kerjasama antara sektor privat dan publik dalam menghadapi ancaman siber yang semakin meningkat. Salah satu model yang dapat diimplementasikan dalam kerjasama ini adalah model hub and spoke dimana sektor privat menjadi anggota (spoke) dan sektor publik menjadi hub. Tantangan terbesar dalam mengimplementasikan model hub and spoke adalah perlunya skema yang dapat memberikan jaminan kepercayaan dalam proses berbagi informasi. Makalah ini mengusulkan skema berbagi informasi keamanan siber menggunakan model hub and spoke yang dapat memberikan jaminan kepercayaan diantara anggotanya. Untuk mencapai jaminan tersebut diusulkan sebuah skema dengan memanfaatkan berbagai teknik kriptografi seperti autenticated encryption dan group signature yang dapat memberikan jaminan kerahasiaan, integritas, keaslian, non-penyangkalan dan perlindungan privasi dalam sebuah skema terintegrasi. Skema ini memiliki kelebihan dimana pemilihan algoritma kriptografi dapat disesuaikan dengan kebutuhan sistem. Hasil pengujian skema dengan menggunakan analisis keamanan menunjukkan skema yang diusulkan memenuhi persyaratan keamanan yang diharapkan. Selain itu dilakukan juga analisis formal menggunakan Scyther Tools untuk menguji ketahanan skema terhadap serangan siber. Hasil analisis formal menunjukkan skema yang diusulkan tahan terhadap berbagai kemungkinan serangan siber.

Kata kunci: keamanan siber, kerahasiaan, protokol kriptografi, *scyther tools*, skema berbagi informasi

1. PENDAHULUAN

Berbagi informasi keamanan siber merupakan salah satu upaya menghadapi tantangan ancaman siber yang semakin meningkat [1-4]. Kerjasama ini pertama kali diperkenalkan oleh Pemerintah Amerika Serikat pada tahun 1990-an antara sektor swasta, antara sektor publik, atau antara sektor publik dan sektor swasta [5]. Terdapat tiga model dalam berbagi informasi, yaitu *hub and spoke*, *post to all* dan *hybrid* [6]. Salah satu model yang dapat diterapkan dalam *public-private partnership* (PPP) adalah *hub and spoke*. Pada model ini, sektor publik berperan sebagai *hub* dan organisasi swasta berperan sebagai *spokes* [7]. Keuntungan dari skema ini adalah informasi yang dibagikan memiliki validitas yang tinggi, namun juga memiliki tantangan terkait dengan kebutuhan *trust* yang tinggi dari anggotanya [8]. Tantangan lain terkait dengan privasi pemilik informasi [4, 9-11]. Beberapa anggota grup *Cybersecurity Information Sharing* (CIS) ingin berbagi informasi namun tidak ingin identitasnya diketahui karena berkaitan dengan reputasi organisasi [12]. Salah satu upaya untuk mendapatkan kepercayaan adalah dengan mengembangkan skema berbagi informasi keamanan siber yang memenuhi beberapa aspek keamanan seperti kerahasiaan, integritas, ketersediaan, *non-repudiation* dan jaminan privasi pemilik informasi.

Beberapa penelitian telah dilakukan untuk memberikan solusi skema berbagi informasi yang memberikan jaminan kerahasiaan, ketersediaan, *non-repudiation* dan jaminan pelindungan privasi. Untuk menjamin kerahasiaan informasi, penelitian dilakukan dengan menerapkan teknik-teknik tertentu seperti pada [13] yang menerapkan kontrol akses untuk membatasi penggunaan informasi dalam kelompok. Penelitian kemudian dikembangkan dengan menambahkan aspek jaminan kerahasiaan dan privasi data [14]. Penelitian lain dilakukan dengan memodifikasi Structured Threat Information Expression (STIX) dengan menambahkan jaminan privasi menggunakan *homomorphic encryption* [15].

Beberapa teknik lain digunakan untuk menjamin privasi pemilik informasi adalah dengan menerapkan anonimitas pengirim informasi. Pada [16] dilakukan pengembangan skema yang memungkinkan organisasi untuk berbagi informasi secara anonim dan memberikan *reward* bagi pengirim informasi. Penelitian dengan menerapkan *permissioned blockchain* untuk menjamin privasi dan kontrol akses dilakukan pada [17]. Pada [18, 19] digunakan skema *forward secrecy* untuk menjamin keamanan berbagi data secara anonim. Metode lain yang digunakan adalah dengan menerapkan *Symmetric Balanced Incomplete Block Design* (SBIBD) [20] dan penggunaan metode *eliptic curve cryptography* [21].

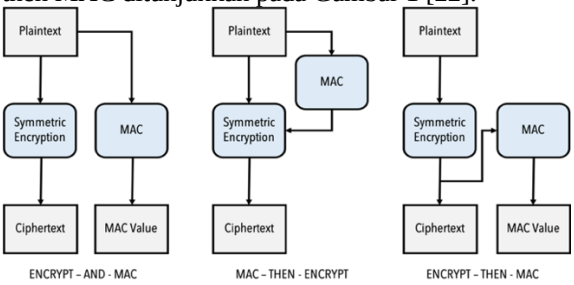
Berdasarkan berbagai penelitian sebelumnya, berbagai metode telah dikembangkan untuk menghasilkan skema CIS yang dapat memberikan jaminan keamanan dan perlindungan privasi. Namun belum ada yang mengusulkan skema yang dapat memberikan seluruh jaminan tersebut dalam sebuah skema yang terintegrasi. Di sisi lain, implementasi berbagi informasi harus dilakukan secara efektif dan efisien. Berdasarkan rumusan masalah di atas maka penelitian ini bertujuan untuk mengembangkan skema

berbagi informasi keamanan siber yang dapat memberikan jaminan kerahasiaan, integritas, autentikasi, nirsangkal dan jaminan perlindungan privasi dalam satu skema serta melakukan pengujian pada skema yang diusulkan menggunakan analisis keamanan dan analisis formal untuk mengukur keamanan terhadap kemungkinan serangan siber.

2. LANDASAN TEORI

2.1. *Authenticated Encryption*

Authenticated Encryption (AE) merupakan teknik kriptografi yang sekaligus dapat menjamin kerahasiaan dan autentikasi pesan [22]. Secara umum, AE dapat dibangun dengan menggabungkan skema enkripsi dan *Message Authentication Code* (MAC) Secara umum, ada tiga pendekatan utama dalam menggabungkan skema enkripsi dan autentikasi yaitu MAC and Encrypt, MAC then Encrypt, dan Encrypt then MAC ditunjukkan pada Gambar 1 [22].

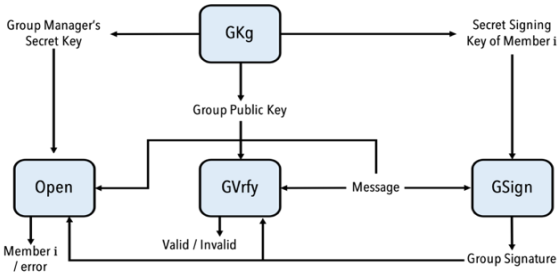


Gambar 1. Authenticated Encryption [22]

2.2. *Group Signature*

Group Signature pertama diperkenalkan oleh Chaum dan Van Heyst dengan mengadopsi proses autentikasi berbasis grup untuk mencapai privasi penandatangan [28]. Skema ini menerapkan gagasan bahwa semua anggota dapat mengeluarkan tanda tangan atas nama seluruh kelompok. Sifat penandatangan grup dapat diverifikasi secara publik menggunakan kunci publik dari semua anggota yang memberikan anonimitas penandatangan. Namun, ada satu pihak tepercaya yang dapat mengaitkan tanda tangan kelompok dengan identitas asli penandatangan. Arsitektur *group signature* terdiri dari *Group Manager* (GM) dan beberapa anggota. GM dapat berupa otoritas tunggal atau kombinasi dari beberapa entitas yang bertanggung jawab atas inisiasi, penerimaan, dan pencabutan kelompok anggota.

Group Signature diklasifikasikan berdasarkan fungsinya, yaitu *Static Group Signature* dan *Dynamic Group Signature*. Skema yang diusulkan menerapkan *Static Group Signature*. Pada skema ini jumlah anggota dalam grup diasumsikan statis sejak proses inisialisasi. Skema ini terdiri dari beberapa algoritme antara lain *Key Generation, Signature Generation, Signature Verification,* dan *Opening Procedure* yang ditunjukkan pada Gambar 2.



Gambar 2. Static Group Signature [22]

3. METODE PENELITIAN

Tahapan penelitian diawali dengan penyusunan *design goals* dari skema yang diharapkan untuk menghasilkan skema yang tepercaya, antara lain:

- Jaminan Privasi: Skema dapat menjamin anonimitas pengirim informasi. Hal ini diwujudkan dengan menerapkan anonimitas di setiap fase.
- Jaminan Kerahasiaan dan Integritas Data: Skema harus menjamin kerahasiaan dan integritas informasi. Hal ini diwujudkan dengan menerapkan algoritma kunci simetris dan *Message Authentication Code* (MAC).
- Jaminan Autentikasi: Skema harus memastikan bahwa informasi dibuat oleh pihak yang memiliki entitas yang tepat. Hal ini akan diwujudkan dengan menggunakan tanda tangan secara anonim.
- Jaminan *Nirsangkal* dan *Traceability*: Skema harus memungkinkan manajer grup untuk membuktikan pemilik informasi dalam kondisi khusus dan tidak dapat menyangkal. Ini akan diwujudkan dengan *group signature*.

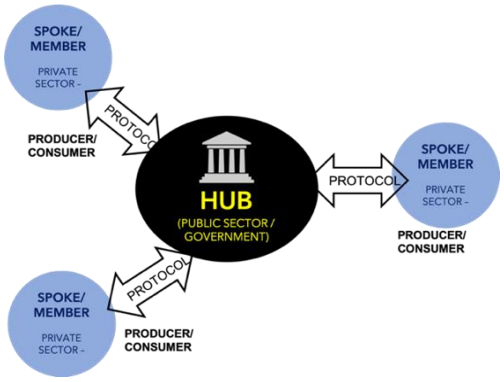
Setelah menentukan *design goals* kemudian diusulkan model berbagi informasi termasuk pembagian tugas dari setiap entitasnya. Dari usulan model tersebut kemudian diusulkan sebuah skema yang dapat memberikan jaminan keamanan yang diharapkan. Tahap berikutnya adalah dengan melakukan pengujian dengan analisis keamanan dan analisis formal. Analisis formal dilakukan menggunakan *Scyther Tools* dengan pengkodean SPDL (*Security Protocol Description Language*). *Tools* ini digunakan untuk mengevaluasi aspek kerahasiaan skema yang diusulkan. Pemilihan *Scyther Tools* dengan alasan mudah digunakan, dapat melakukan verifikasi dengan cepat, dan telah digunakan dalam banyak penelitian. *Tools* ini diinstal pada mesin Ubuntu OS 20.04 dengan memori 4GB.

4. HASIL DAN PEMBAHASAN

4.1. Usulan Model *Hub and Spoke*

Model yang diusulkan terdiri dari dua entitas, yaitu *Hub* dan *Member*. *Hub* memiliki dua tugas yaitu sebagai, *Group Manager* (GM) dan *hub* informasi.

Sebagai GM, *hub* menerima pendaftaran *member*, membangkitkan dan mendistribusikan kunci, serta mengelola grup. Sebagai *hub* informasi, *hub* memiliki tugas menerima informasi, memverifikasi keabsahan *group signature*, dan mendistribusikan informasi yang valid kepada anggota lain. Dalam implementasinya, *hub* adalah organisasi sektor publik. *Member* adalah entitas dalam grup yang dapat bertindak sebagai *Information Produce Organization* (IPO) atau *Information Receive Organization* (IRO). Sebagai IPO, *member* dapat berkontribusi memberikan informasi kepada anggota lain melalui *hub*. Sebagai IRO, *member* menerima informasi terverifikasi dari *hub*. *Member/spoke* adalah organisasi sektor swasta atau kelompok tertentu yang memiliki profil serupa di bidang keamanan siber. Usulan model dalam skema berbagi informasi disajikan dalam Gambar 3.



Gambar 3. Usulan Model Hub and Spoke [diolah sendiri]

4.2. Usulan Skema CIS

Usulan skema dirancang menggunakan beberapa teknik kriptografi seperti AE dan *group signature*. Teknik-teknik kriptografi tersebut disusun sebagaimana sehingga menghasilkan skema berbagi informasi keamanan siber yang dapat memberikan jaminan sesuai dengan *design goals* yang diharapkan sebagaimana terlihat pada Gambar 4. Pada algoritme AE, skema menggunakan pendekatan Encrypt then MAC. Skema yang diusulkan ditunjukkan pada Gambar 4. Pada usulan skema terdapat 6 fase antara lain: (1) fase registrasi (2) fase pembangkitan kunci, (3) fase pengiriman informasi, (4) fase verifikasi, (5) fase penerimaan informasi, dan (6) fase *dispute*. Penjelasan notasi yang digunakan pada skema dapat dilihat pada Tabel 1.

Tabel 1. Notasi

Notasi	Definisi
$\boldsymbol{M}$	Informasi keamanan siber
$\boldsymbol{K = \{K_1, \ldots, K_m\}}$	*Master Key*
$\boldsymbol{m}$	Jumlah *master key* yang dibangkitkan
$\boldsymbol{n}$	Panjang master key
$\boldsymbol{o}$	Panjang GM *Daily Token*
$\boldsymbol{a}$	Bilangan acak diantara $1 - m$, dalam *Scyther* dinotasikan dengan *Ni*
$\boldsymbol{h}(.)$	Nilai *hash* dengan input (.)
$(\boldsymbol{CT_d})$	*Central Hub Daily Token*
$\boldsymbol{DEK}$	*Data Encrypting Key*
$\boldsymbol{DAK}$	*Data Authentication Key*
$\boldsymbol{E}(.)$	Proses enkripsi pada suatu input (.)
$\boldsymbol{MAC}(.)$	Hasil perhitungan MAC pada input (.)
$\|$	Operasi konkatenasi
$\boldsymbol{GKg}$	KeyGen Algorithm pada *Group Signature*
$\boldsymbol{GSign}$	*Sign Algorithm* pada *Group Signature*
$\boldsymbol{GVrfy}$	*Verify Algorithm* pada *Group Signature*
$\boldsymbol{Open}$	*Open Algorithm* pada *Group Signature*

4.2.1. Fase Registrasi

Proses registrasi dilakukan oleh setiap anggota yang akan bergabung dengan grup secara sukarela. Dalam pelaksanaannya, proses registrasi dilakukan oleh *hub* yang merupakan organisasi publik atau yang berfungsi sebagai *regulator* di sektor tertentu. Proses pendaftaran tidak dilakukan secara anonim untuk mengecek kriteria dan persyaratan yang dibutuhkan. Kemudian *hub* menghitung jumlah total anggota guna menentukan parameter yang dibutuhkan.

4.2.2. Fase Pembangkitan Kunci

Pada fase ini, kunci simetris dan asimetris dibangkitkan. Kunci simetris digunakan untuk melakukan AE, sedangkan kunci asimetris digunakan untuk *group signature*. Proses pembangkitan kunci simetris dilakukan oleh *hub* pada awal pembentukan grup dengan tahapan sebagai berikut:

- Bangkitkan bilangan acak $K = \{K_1, \ldots, K_m\}$ sebanyak n-bit untuk *Master Key*. n menunjukkan panjang bit kunci sedangkan m menunjukkan jumlah kunci yang dihasilkan.
- Hitung nilai hash MK $(h(K))$ menggunakan algoritma fungsi hash yang disepakati.
- Bagikan MK dengan $(h(K))$ kepada anggota.
- Anggota menerima nilai MK dan $(h(K))$ kemudian menghitung nilai $(h(K)')$ menggunakan algoritma yang disepakati, jika nilai $(h(K))$ dan $(h(K)')$ sama, integritas dari informasi dijamin.

Kunci asimetris dihasilkan untuk proses *group signature* dengan proses yang disepakati dalam grup. Pada *group signature*, ada tiga jenis kunci yang dihasilkan oleh GM, Kunci Privat Anggota untuk dalam proses *group signature*, Kunci Publik Grup untuk proses verifikasi, dan Kunci Privat GM untuk proses dalam tahap *dispute*.

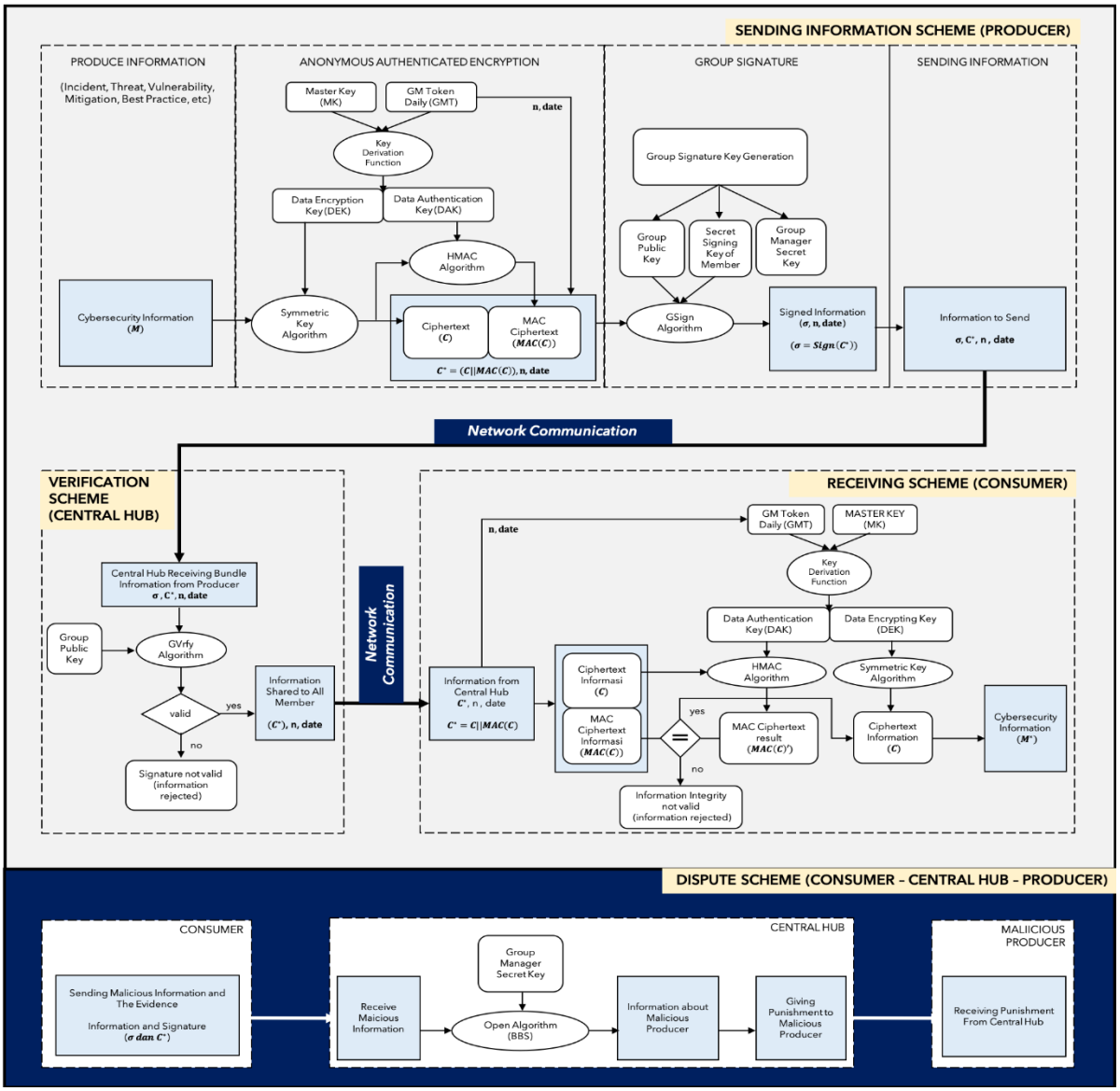
4.2.3. Fase Pengiriman Informasi

Proses ini adalah pengiriman informasi dari IPO ke *Hub*. Skema ini terdiri dari tiga bagian, yaitu *Key Derivation*, *Cryptographic Process*, dan *Network Communication*. Pada tahap *key derivation*, IPO melakukan langkah ini:

- Unduh *Central Hub Daily Token* (CT_d) dari platform yang disetujui oleh grup. Token ini akan berubah setiap hari dan berisi o-bit dengan panjang yang sama dengan MK (n-bit).
- Pilih bilangan acak a antara 1 sampai m.
- Gunakan n-bit bilangan acak a dari *file* yang berisi

bilangan acak (K_m).

- Hitung $DEK = Hash\ (K_m||GMT_d)$, Hash adalah fungsi hash seperti SHA-256.
- Hitung $DAK = E(DEK, DEK)$, E adalah algoritme simetris misalnya AES-256.



Gambar 4. Usulan Skema CIS

Dalam *cryptographic process*, pertama-tama lakukan AE untuk mewujudkan kerahasiaan dan integritas. Informasi dienkripsi dengan algoritma kunci simetris menggunakan DEK. Algoritma dapat dipilih sesuai kebutuhan, misalnya Algoritma AES. *Ciphertext* terenkripsi kemudian dihitung nilai MAC-nya menggunakan algoritma HMAC dan DAK. *Ciphertext*, nilai MAC, parameter a, dan tanggal pengiriman informasi kemudian digabungkan menjadi sekumpulan informasi yang disebut (C^*). Langkah kedua adalah *Anonymous Group Signature* untuk mencapai autentikasi, nirsangkal. Pesan ditandatangani menggunakan inputan berupa kunci publik grup, kunci privat anggota, dan pesan (C^*). Penandatanganan pesan dilakukan dengan memilih parameter sesuai algoritma masing-masing. Output tahap ini adalah *signature*. Kemudian (C^*) dan *signature*-nya siap untuk ditransmisikan ke Hub. Skema ini menggunakan *Static Group Signature*. Pada skema in algoritme dapat dipilih sesuai kebutuhan, misalnya BBS *Group Signature.* Proses protokol ini disebut dengan nama $CIS1$.

Dalam *Network Communication*, pesan akan dikirim dari IPO ke *Hub* dan dari *Hub* ke IRO. Tahap ini penting karena jika komunikasi jaringan dapat dianalisis, maka skema anonim tidak akan efektif. Proses anonimitas jaringan tidak termasuk dalam ruang lingkup penelitian.

4.2.4. Fase Verifikasi Informasi

Hub bertugas menerima informasi dari IPO, memverifikasi otoritas entitas, dan mendistribusikan

informasi tersebut ke IRO. Tahapan dimulai ketika *Hub* menerima bundel informasi yang telah ditandatangani pengirim dengan algoritme $Sign$ kemudian Hub menjalankan algoritme $GVrfy$ menggunakan kunci publik grup (gpk), menginput pesan dan *group signature* yang dikirim serta memverifikasi kebenaran *group signature* yang dikirim oleh pengirim. Jika tanda tangan tidak valid, informasi akan diabaikan. Jika hasil verifikasi valid, informasi tersebut akan didistribusikan ke seluruh anggota grup dalam bentuk bundel informasi (C^*).

4.2.5. Fase Penerimaan Informasi

Langkah ini dilakukan ketika IRO menerima informasi dari Hub. Bundel informasi (C^*) berisi *ciphertext*, nilai MAC, parameter a, dan tanggal pengiriman untuk kemudian mendekripsi pesan dan memeriksa integritas informasi. Tahap dekripsi pesan diawali dengan perhitungan kunci simetris dengan langkah yang dilakukan sama dengan tahapan pembuatan kunci simetris oleh pengirim informasi:

- Menggunakan nilai a untuk mengambil 256-bit angka bilangan ke m dari file bilangan acak (K_m).
- Membaca informasi tanggal pengiriman dan menggunakan token GMT_d untuk menghasilkan DEK dan DAK.
- Hitung $DEK = Hash\,(K_n||GMT_d)$, *Hash* adalah fungsi hash misalnya SHA-256.
- Hitung $DAK = E(DEK, DEK)$, E adalah algoritma simetris misalnya AES-256.

Setelah mendapatkan nilai DEK dan DAK, kemudian menghitung nilai MAC pesan dengan input *ciphertext* dan DAK. Bandingkan hasil MAC dengan MAC yang diperoleh dari bundel informasi (C^*). Jika nilai MAC berbeda, integritas pesan tidak dijamin sehingga informasi diabaikan. Jika nilai MAC sama, dilanjutkan dengan dekripsi pesan menggunakan DEK. Protokol ini disebut sebagai protokol $CIS2$.

4.2.6. Skema Dispute

Skema CIS yang diusulkan juga dapat dieksploitasi oleh entitas yang berperilaku jahat. Entitas yang tidak bertanggung jawab dapat mengirimkan informasi berbahaya kepada entitas lain. Untuk mencegahnya, skema tersebut harus mendukung kemungkinan *Hub* mengetahui identitas asli pengirim informasi dalam kondisi tertentu (*traceable*). Jika hal ini dapat dipenuhi, maka skema juga dapat memberikan jaminan nirsangkal, pengirim informasi tidak dapat menyangkal bahwa dia telah mengirimkan informasi. Persyaratan ini dapat diwujudkan dalam *Group Signature* yang digunakan pada tahap penandatanganan pesan. Ketika menemukan informasi berbahaya, entitas dapat memulai proses pengungkapan identitas ke *Hub* dengan mengirimkan informasi bersama dengan bukti dalam bentuk pesan dan tanda tangan yang sesuai kepada GM. Kebijakan mengenai informasi berbahaya apa pun akan dimuat dalam kebijakan CIS. Setelah mendapatkan informasi terkait informasi berbahaya, GM menjalankan algoritma $Open$ pada *Group Signature* dengan input berupa kunci publik grup, kunci rahasia GM, pesan, dan tanda tangan. Algoritma ini digunakan untuk melakukan pelacakan tanda tangan untuk menandatangani pesan. Proses ini hanya dapat dilakukan oleh GM karena memiliki parameter input $GM\ Secret\ Key$. Sanksi dalam kondisi ini dapat diatur dalam kebijakan grup CIS.

4.3. Analisis Keamanan

4.3.1. Privasi Pengguna

Skema yang diusulkan menjamin privasi pengguna dengan menerapkan anonimitas pada setiap tahap berbagi informasi. Pada tahap inisiasi, Hub bertugas untuk membangkitkan bilangan acak $\boldsymbol{K} = \{\boldsymbol{K_1}, \ldots, \boldsymbol{K_m}\}$ sepanjang n-bit yang akan dijadikan Master Key (MK) sebanyak m yang kemudian didistribusikan ke semua anggota. MK yang dibagikan seluruhnya sama untuk setiap anggota sehingga MK tidak menunjukkan identitas pengguna. Untuk menjamin keamanan informasi, kunci yang akan digunakan untuk proses AE akan berbeda untuk setiap proses pengiriman informasi. Hal ini dapat dicapai karena adanya proses pemilihan parameter secara acak yang menunjukkan MK yang digunakan untuk diproses pada tahap *Key Derivation*. Proses *Key Derivation* dilakukan oleh IPO dan seluruh *member* saat mengirim informasi dan menerima informasi dari *Central Hub*. Parameter yang dibutuhkan antara lain *Master Key* (K), dan bilangan acak (a) yang menunjukkan Master Key yang dipilih.

Key, GM Daily Token GMT_d dan tanggal, tidak ada yang menunjukkan identitas IPO karena semua parameter bersifat umum. Kemudian parameter diolah dengan algoritme *Key Derivation* untuk kemudian menjadi DEK dan DAK untuk proses AE. Hal ini membuktikan bahwa tahap AE dilakukan secara anonim. Dalam *group signature*, anonimitas penanda tangan menjadi fitur inti yang menunjukkan bahwa tidak ada pihak selain GM yang dapat mengidentifikasi penanda tangan *group signature*.

4.3.2. Kerahasiaan dan Integritas Data

Proses AE mewujudkan skema CIS yang menjamin kerahasiaan dan integritas informasi tetapi tetap memastikan perlindungan privasi. Dalam skema yang diusulkan, pendekatan AE yang digunakan adalah *Encrypt then MAC*. Pendekatan ini dapat mencapai tingkat keamanan tertinggi pada AE.

4.3.3. Autentikasi

Proses *Group Signature* dilakukan untuk mencapai autentikasi informasi. Skema ini menjamin bahwa informasi hanya dapat dibuat oleh pihak yang memiliki kunci rahasia melalui proses $Sign$ dari *group signature*. Proses autentikasi dilakukan oleh *Hub* baru kemudian informasi dibagikan kepada IRO.

4.3.4. Nirsangkal dan *Traceability*

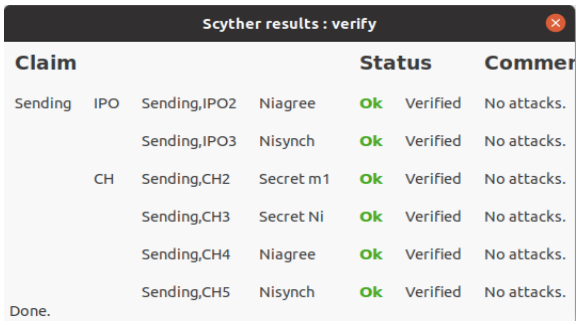
Skema ini memungkinkan *Hub* untuk mengetahui identitas pengirim informasi dalam kondisi tertentu. Jika hal ini dipenuhi, maka skema juga memberikan jaminan nirsangkal. Ketika menemukan informasi berbahaya, entitas dapat memulai proses pengungkapan identitas (*dispute*) ke *Hub* dengan mengirimkan informasi beserta bukti berupa pesan dan tanda tangan terkait kepada GM. Kemudian, GM menjalankan algoritme *Open* pada *Group Signature* dengan input berupa kunci publik grup, kunci rahasia GM, pesan, dan tanda tangan. Algoritme ini digunakan untuk melakukan pelacakan tanda tangan. Proses ini hanya dapat dilakukan oleh GM karena memiliki parameter input GM *Secret Key*.

4.4. Analisis Formal

Scyther Tools digunakan untuk memvalidasi protokol yang diusulkan menggunakan analisis formal. Pada evaluasi ini dilakukan dalam dua protokol yaitu $CIS1$ dan $CIS2$ yang didefinisikan dalam Bagian 4.2.

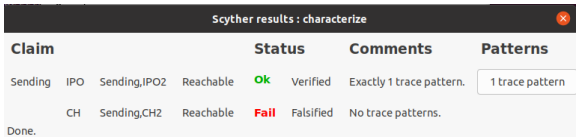
4.4.1. Verifikasi Keamanan $CIS1$

Hasil analisis formal $CIS1$ menunjukkan bahwa $CIS1$ memberikan jaminan kerahasiaan pada $m1$ dan Ni. Selain itu, $CIS1$ juga dirancang untuk memenuhi Nisynch dan Niagree yang berarti bahwa setiap komunikasi dalam protokol berjalan dalam pertukaran data yang benar. Hasil verifikasi menunjukkan bahwa tidak ada kemungkinan serangan dalam protokol komunikasi antara IPO dan CH seperti yang ditunjukkan pada Gambar 5.



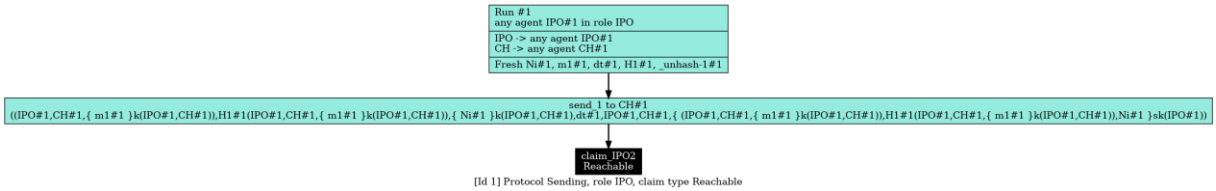
Gambar 5. Hasil Verifikasi CIS1

Hasil pengujian menunjukkan pola komunikasi antara IPO dan CH. Hasil ini menunjukkan bahwa terdapat satu *trace* dengan status OK pada IPO yang menunjukkan bahwa arus komunikasi berjalan satu arah dari IPO ke CH seperti terlihat pada Gambar 6.



Gambar 6. Hasil Pattern CIS1

Saat hasil pola *trace* dibuka, maka akan terlihat kemungkinan adanya *trace* antara IPO dan CH seperti terlihat pada Gambar 7. Gambar 7 menunjukkan jalur komunikasi yang terjadi pada protokol $CIS1$ antara IPO dan CH. Hasil ini juga menunjukkan bahwa protokol $CIS1$ dapat diimplementasikan sebagai protokol komunikasi.

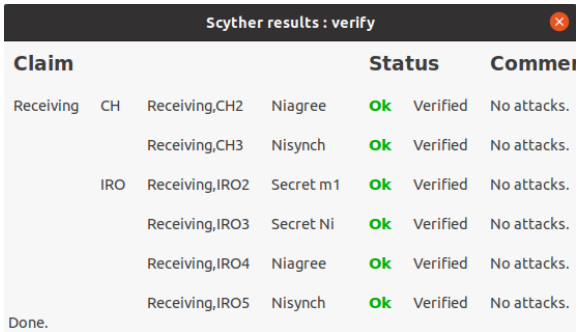


Gambar 7. Protocol $CIS1$, Role IPO, *Claim Type Reachable*

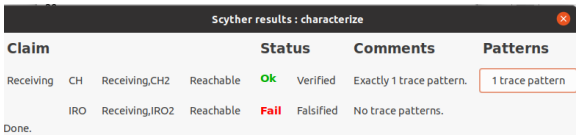
4.4.2. Verifikasi Keamanan $CIS2$

Hasil analisis formal $CIS2$ menunjukkan bahwa $CIS2$ memberikan jaminan kerahasiaan pada $m1$ dan Ni. $CIS2$ juga dirancang untuk memenuhi Nisynch dan Niagree yang berarti komunikasi dalam protokol berjalan dalam pertukaran data yang benar. Hasil verifikasi menunjukkan tidak ada kemungkinan serangan dalam protokol komunikasi antara CH dan IRO seperti yang ditunjukkan pada Gambar 8.

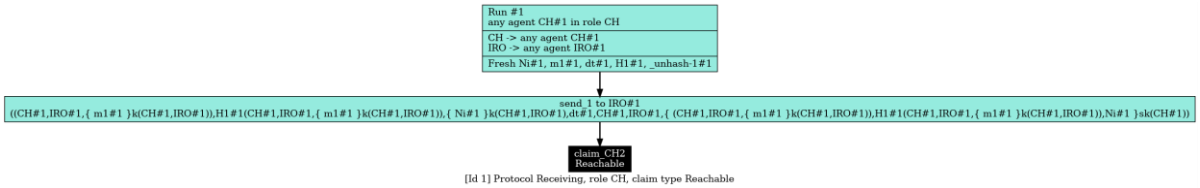
Hasil pengujian menunjukkan pola komunikasi antara CH dan IRO. Hasil ini menunjukkan bahwa terdapat satu *trace* dengan status OK pada CH yang menunjukkan bahwa arus komunikasi berjalan satu arah dari CH ke IRO seperti terlihat pada Gambar 9.



Gambar 8. Hasil Verifikasi $CIS2$



Gambar 9. Hasil *Pattern* $CIS2$



Gambar 10. Protocol ***CIS2***, Role IRO, *Claim Type Reachable*

Trace pattern menunjukkan adanya *trace* antara CH dan IRO seperti terlihat pada Gambar 10. Gambar 10 menunjukkan jalur komunikasi yang terjadi pada protokol $CIS2$ antara CH dan IRO. Hasil ini juga menunjukkan bahwa protokol $CIS2$ dapat diimplementasikan sebagai protokol komunikasi.

4.5. Diskusi

Untuk mewujudkan skema yang benar-benar menjamin anonimitas, tantangan lain perlu dipenuhi, seperti anonimitas jaringan dalam transaksi informasi. Komunikasi dalam jaringan juga penting karena berbagai teknik anonimitas tidak akan efektif jika jaringan yang digunakan dapat mengungkap identitas pengirim. Beberapa teknik dapat digunakan untuk membuat jaringan anonim, misalnya dengan menggunakan *server proxy untuk* mengirimkan informasi. Salah satu implementasi dari *server proxy* adalah Tor yang dapat mencapai anonimitas jaringan.

Tantangan lain adalah memastikan isi pesan yang dikirim tidak mengandung informasi yang dapat mengungkap identitas pengirim. Berbagai teknik dapat digunakan untuk menganonimkan isi pesan, mulai dari prosedur sederhana yang mengharuskan pemilik informasi menghapus semua hal yang berkaitan dengan identitas pengirim atau proses sanitasi pesan otomatis.

Kekuatan skema ini juga tergantung pada pemilihan algoritma tertentu yang akan digunakan dalam pemrosesan informasi. Secara umum ada tiga algoritma yang dapat dipilih saat mengimplementasikan skema ini, antara lain algoritme kunci simetris untuk proses enkripsi, algoritme HMAC untuk proses *hashing*, keduanya digunakan pada proses AE dan *algoritme* ketiga adalah algoritme *group signature*. Pada algoritme simetris, kekuatan algoritme tergantung pada faktor seperti kerahasiaan kunci kriptografi itu sendiri. Penyerang juga akan mencoba menebak kunci dengan berbagai cara sehingga panjang kunci juga akan mempengaruhi keamanan algoritma. Semakin lama kunci digunakan, semakin sulit bagi penyerang untuk menebak kuncinya. Skema ini juga dimungkinkan untuk diimplementasikan menggunakan algoritme *proprietary* sehingga kelompok CIS dapat mengimplementasikan algoritme independen daripada menggunakan algoritme standar. Dalam implementasinya, pemilihan algoritme *group signature* juga dapat disesuaikan dengan kebutuhan grup. Pemilihan ini dapat didasarkan pada kemampuan komputasi dari masing-masing platform yang akan digunakan dalam implementasi skema yang diusulkan.

Keuntungan dari skema yang diusulkan adalah memiliki jaminan keamanan kriptografi yang lengkap termasuk kerahasiaan, integritas, autentikasi dan nirsangkal yang diwujudkan melalui AE dan *group signature*. Keuntungan lainnya adalah jaminan keamanan di atas juga diterapkan dalam lingkungan yang melindungi keamanan privasi melalui penerapan anonimitas di setiap tahap tetapi juga mendukung ketertelusuran dalam kondisi tertentu. Dengan semua keunggulan tersebut, skema yang diusulkan akan cocok jika diterapkan dalam lingkungan kemitraan publik-swasta. Perbandingan skema yang diusulkan dan berbagai skema berbagi informasi ditunjukkan pada Tabel 2.

Tabel 2. Perbandingan dengan Skema Lain

Skema	Aspek Keamanan					
	1	2	3	4	5	6
I. Vakilinia, et al. [13]	-	✓	-	✓	-	-
I. Vakilinia et, al. [16]	✓	-	-	✓	✓	✓
F. Sadique, et al. [14]	✓	✓	✓	✓	✓	-
Z. Fathi, et al. [17]	✓	-	✓	✓	-	-
J. Shen, et al. [20]	✓	✓	-	✓	✓	✓
Usulan Skema	✓	✓	✓	✓	✓	✓

(1) *User Privacy*, (2) *Confidentiality*, (3) *Integrity*,
(4) *Authentication*, (5) *Non Repudiation*, (6) *Traceability*

5. KESIMPULAN

Makalah ini mengusulkan skema CIS untuk PPP menggunakan model *Hub and Spoke* yang menghubungkan IPO dan IRO di sektor privat melalui organisasi publik yang dikenal sebagai *Hub*. Skema berfokus pada penyediaan skema tepercaya untk berbagi informasi yang diwujudkan dengan menggunakan teknik kriptografi yaitu AE dan *group signature.* AE menjamin kerahasiaan dan integritas dalam satu proses, sedangkan *group signature* menjamin autentikasi, nirsangkal, dan *traceability.* Skema ini memberikan keleluasaan dalam proses implementasi algoritma yang dapat disesuaikan dengan kebutuhan sistem. Hasil analisis formal dengan *Scyther tools* membuktikan bahwa skema tahan terhadap kemungkinan serangan siber. Hasil analisis keamanan menunjukkan bahwa skema memberikan jaminan yang diperlukan untuk menghasilkan skema yang tepercaya. Keterbatasan

penelitian ini adalah skema yang diusulkan hanya dapat diterapkan pada grup statis sehingga tidak memungkinkan untuk menambah anggota ketika skema telah berjalan.

Penelitian ini masih terbuka untuk dilakukan dilanjutkan dalam beberapa aspek, misalnya terkait implementasi skema dengan perbandingan menggunakan pemilihan algoritme tertentu. Penelitian selanjutnya dapat mengevaluasi kinerja skema dengan menggunakan berbagai jenis algoritme AE serta *group signature*. Penelitian juga dapat dikembangkan dengan mengubah skema *group signature* statis menjadi *group signature* dinamis yang memungkinkan penambahan anggota selama CIS berjalan. Penelitian selanjutnya juga dapat mengimplementasikan skema ini pada platform tertentu dengan menerapkan sistem otomatisasi sehingga skema CIS dapat berjalan lebih cepat. Skema ini diharapkan dapat bermanfaat dalam untuk mewujudkan *cybersecurity situational awareness*, khususnya dalam lingkup *public-private partnership*.

REFERENSI

[1] E. Luijijf and A. Kernkamp, "Sharing Cyber Security Information - Good Practice from the Dutch Public Private Participation Approach," 2015.

[2] W. Zhao and G. White, "A collaborative information sharing framework for Community Cyber Security," in *2012 IEEE Conference on Technologies for Homeland Security (HST)*, 13-15 Nov. 2012 2012, pp. 457-462, doi: 10.1109/THS.2012.6459892.

[3] K. Fotiadou, T. H. Velivassaki, A. Voulkidis, K. Railis, P. Trakadas, and T. Zahariadis, "Incidents Information Sharing Platform for Distributed Attack Detection," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 593-605, 2020, doi: 10.1109/OJCOMS.2020.2989925.

[4] P. Naghizadeh and M. Liu, "Using Private and Public Assessments in Security Information Sharing Agreements," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1801-1814, 2020, doi: 10.1109/TIFS.2019.2950125.

[5] S. Ghernaouti, L. Cellier, and B. Wanner, "Information sharing in cybersecurity : Enhancing security, trust and privacy by capacity building," in *2019 3rd Cyber Security in Networking Conference (CSNet)*, 23-25 Oct. 2019 2019, pp. 58-62, doi: 10.1109/CSNet47905.2019.9108944.

[6] MITRE, "Cyber Information-Sharing Models : An Overview," *MITRS*, 2012.

[7] (2017). *Public Private Partnership - Cooperative Models*.

[8] K. Harrison and G. White, "Information sharing requirements and framework needed for community cyber incident detection and response," in *2012 IEEE Conference on Technologies for Homeland Security (HST)*, 13-15 Nov. 2012 2012, pp. 463-469, doi: 10.1109/THS.2012.6459893.

[9] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 331-346, 2019, doi: 10.1109/TIFS.2018.2850312.

[10] L. Nweke and S. Wolthusen, *Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection*. 2020.

[11] R. Jin, X. He, and H. Dai, "On the Security-Privacy Tradeoff in Collaborative Security: A Quantitative Information Flow Game Perspective," *Trans. Info. For. Sec.*, vol. 14, no. 12, pp. 3273–3286, 2019, doi: 10.1109/tifs.2019.2914358.

[12] T. Kokkonen, J. Hautamäki, J. Siltanen, and T. Hämäläinen, "Model for sharing the information of cyber security situation awareness between organizations," in *2016 23rd International Conference on Telecommunications (ICT)*, 16-18 May 2016 2016, pp. 1-5, doi: 10.1109/ICT.2016.7500406.

[13] I. Vakilinia, D. K. Tosh, and S. Sengupta, "Attribute based sharing in cybersecurity information exchange framework," in *2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, 9-12 July 2017 2017, pp. 1-6, doi: 10.23919/SPECTS.2017.8046770.

[14] F. Sadique, K. Bakhshaliyev, J. Springer, and S. Sengupta, "A System Architecture of Cybersecurity Information Exchange with Privacy (CYBEX-P)," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 7-9 Jan. 2019 2019, pp. 0493-0498, doi: 10.1109/CCWC.2019.8666600.

[15] I. Vakilinia, D. Tosh, and S. Sengupta, *Privacy-preserving cybersecurity information exchange mechanism*. 2017, pp. 1-7.

[16] I. Vakilinia, D. K. Tosh, and S. Sengupta, "Privacy-preserving cybersecurity information exchange mechanism," in *2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, 9-12 July 2017 2017, pp. 1-7, doi: 10.23919/SPECTS.2017.8046783.

[17] Z. Fathi, A. J. Rafsanjani, and F. Habibi, "Anon-ISAC: Anonymity-preserving cyber threat information sharing platform based on permissioned Blockchain," in *2020 28th Iranian Conference on Electrical Engineering (ICEE)*, 4-6 Aug. 2020 2020, pp. 1-5, doi: 10.1109/ICEE50131.2020.9261029.

[18] X. Huang *et al.*, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security," *IEEE Transactions on Computers*, vol. 64, no. 4, pp. 971-983, 2015, doi: 10.1109/TC.2014.2315619.

[19] R. Li, H. Asaeda, and J. Li, "A Distributed Publisher-Driven Secure Data Sharing Scheme for Information-Centric IoT," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 791-803, 2017, doi: 10.1109/JIOT.2017.2666799.

[20] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and Traceable Group Data Sharing in Cloud Computing," *IEEE Transactions on Information Forensics and Security*, vol. PP, pp. 1-1, 11/16 2017, doi: 10.1109/TIFS.2017.2774439.

[21] M. A. Will, R. K. L. Ko, and S. J. Schlickmann, "Anonymous Data Sharing Between Organisations with Elliptic Curve Cryptography," in *2017 IEEE Trustcom/BigDataSE/ICESS*, 1-4 Aug. 2017 2017, pp. 1024-1031, doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.347

[22] A. Malek. "Authenticated Encryption." https://superkogito.github.io/blog/AuthenticatedEncryption.html (accessed February 27th, 2022).