Kombinasi Algoritma RSA Dan Algoritma Fuzzy Identity Based Encryption (FIBE) Untuk Mencegah Spear Phishing

Eliando[1], Yunianto Purnomo[2]
eliando.kilapong@matanauniversity.ac.id; yunianto.purnomo@matanauniversity.ac.id
Matana University, ARA Center, Matana University Tower,
Jl. CBD Barat Kav. 1 Gading Serpong, Tangerang - 15810

Abstrak. Phishing adalah sebuah cara untuk mengambil informasi penting seperti username dan password, nomor kartu kredit, social security number, alamat tempat tinggal, email bahkan tanda tangan, yang merupakan identitas baik pribadi maupun sebuah institusi, dan jika informasi tersebut diambil maka akan sangat berbahaya bagi indvidu maupun institusi yang bersangkutan. Untuk melindungi dari serangan phishing banyak cara dapat digunakan, salah satunya adalah dengan mengimplemtasikan algoritma RSA dengan *Fuzzy Identity Based Encryption (FIBE) Algorithm* dengan kombinasi kedua algoritma tersebut serangan phising dapat dihindari, karena kedua algoritma tersebut memiliki karakteristik yang dapat menutup setiap celah keamanan yang ada ketika data, dokumen atau file dikirimkan melalui jaringan.
Kata Kunci: Phishing, RSA, FIBE, Algoritma, Keamanan

1. PENDAHULUAN

Keamanan berbanding terbalik dengan kenyamanan. Seiring dengan meningkatnya nilai aset informasi, keinginan orang untuk mendapatkan akses informasi dan mengendalikannya juga meningkat. Dalam menghadapi usaha perolehan informasi secara ilegal, orang-orang berusaha mencegah tindak kriminal terkait informasi atau berusaha meminimalisasi kerusakan akibat tindak kriminal tersebut. Inilah yang disebut dengan keamanan informasi. Pengamanan informasi diperlukan agar kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (availability) informasi tetap terjaga agar tidak mengganggu kinerja dan operasional organisasi. Kegagalan proses pengamanan informasi akan berefek langsung terhadap kepercayaan pelanggan atau masyarakat yang dampaknya dapat mengganggu hingga membawa bencana bagi institusi bahkan keamanan nasional [1]. Salah satu serangan untuk memperoleh data dan informasi secara ilegal yaitu dengan cara Phising dimana aktivitas seseorang untuk mendapatkan informasi rahasia user dengan cara menggunakan email dan situs web palsu yang tampilannya menyerupai tampilan asli atau resmi web sebenarnya. Informasi yang didapat atau dicari oleh phiser adalah berupa password account atau nomor kartu kredit korban. Penjebak (phisher) menggunakan email, banner atau pop-up window untuk menjebak user agar mengarahkan ke situs web palsu (fake webpage), dimana user diminta untuk memberikan informasi pribadinya. Disinilah phisher memanfaatkan kecerobohan dan ketidak telitian user dalam web palsu tersebut untuk mendapatkan informasi. [2].
Banyak cara untuk mencegah serangan phishing salah satunya dengan penggunaan kunci pribadi dapat digunakan untuk autentikasi (pengenalan identitas pengirim) dan non repudiasi (pencegahan penyangkalan pengiriman data) karena dalam proses dekripsi dapat diketahui siapa pihak pengirim dengan melihat kunci pribadi yang dipakai. Contoh algoritma kriptografi yang dapat dihandalkan adalah RSA, dimana RSA merupakan proses penyandian kunci asimetrik (asymmetric key). Proses perumusan RSA didasarkan pada Teorema Euler, sedemikian sehingga menghasilkan kunci umum dan kunci pribadi yang saling berkaitan. Sehingga meskipun proses enkripsi dan dekripsi menggunakan dua kunci yang berbeda hasilnya akan tetap benar. Kunci umum dan kunci pribadi yang digunakan adalah suatu bilangan prima, dan disarankan bilangan prima yang besar. Hal ini digunakan untuk pencegahan usaha pemecahan teks rahasia, karena semakin besar bilangan prima yang digunakan sebagai kunci maka semakin sulit mencari bilangan besar sebagai faktornya.[3].
Selain RSA terdapat algoritma cryptography baru yang dikenal dengan Identity Based Cryptography (IBC). Skema baru ini akan menyebabkan kinerja yang lebih baik ketika ada permintaan otentikasi simultan menggunakan Verification Batch berbasis Identity. Selanjutnya

menganalisis keamanan protokol baru dan disajikan evaluasi kinerja operasi kriptografinya. [4]. IBC bila dikombinasikan dengan Fuzzy Logic tentu saja akan menghasilkan kombinasi algoritma yang unik dan lebih aman, yang jika dikombinasikan dengan algoritma RSA akan memberikan perlindungan lebih dari serangan phishing, tidak hanya serangan spear phishing tapi juga semua jenis serangan phishing yang lainnya.

1.1.Algoritma RSA

Secara sederhana algoritma RSA dapat dihitung dengan perhitungan sebagai berikut :

1. Pilih dua bilangan prima p dan q secara acak , $p \neq q$.
2. Hitung $N = pq$. Bilangan N disebut parameter keamanan.
3. Hitung $\varphi(N) = (p-1)(q-1)$.
4. Pilih kunci publik, e, yang relatif prima terhadap φ (n).
5. Hitung d hingga $d\ e \equiv 1 \pmod{\varphi}$.

Perhitungan dasar ini digunakan untuk mencari public key dan private key nya, sehingga nilai private key di dapat ketika menghitung public key nya, dengan melihat perhitungan pada algoritma RSA, maka semakin panjang bilangan yang ditentukan makan akan semakin banyak perhitungan yang dihasilkan demikian dengan nilai dari kunci public dan kunci private tersebut, yang dapat disimpulkan bahwa algoritma ini merupakan algoritma yang sangat aman, tanpa adanya kunci private hamper mustahil seseorang untuk melakukan phising maupun pencurian data.

1.2. Algoritma Fuzzy Identity Based

Pada algoritma ini mirip dengan Algoritma *Identity Based Encryption (IDE)* dimana algoritma ini di jalankan oleh sebuah generator atau bisa dikatakan *Private Key Generator(PKG)* yang membuat seluruh algoritma ini bekerja. Generator tersebut membuat kunci private dan kunci publik, dimana kunci publik dikirimkan ke publik atau ke internet, yang nantinya Generator tersebut akan mengeluarkan kunci private ketika ada permintaan dari kunci publiknya, misalkan

1. Diketahui sebuah sistem memiliki parameter *A* dan *P*, dimana didalamnya terdapat pesan atau *M* dan ciphertext atau *C*
2. Diketahui sebuah generator yaitu *Km*

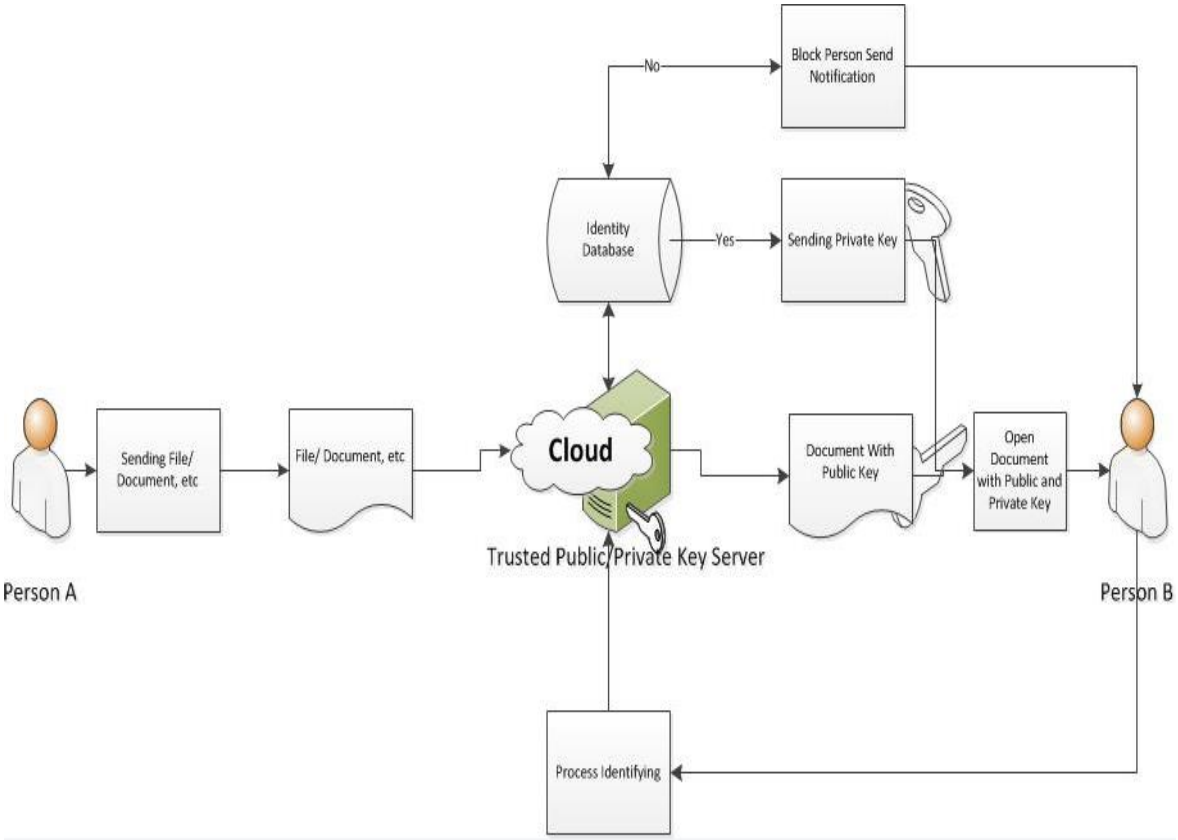
Ketika melakukan ekstraksi yang menggunakan protocol jaringan yang bekerja pada layer transport yang memiliki satu jalur yang bisa disebut *d* sehingga jalur tersebut aman dan protocol tersebut dapat dikenali oleh *A* dan *P*, misalkan input dilakukan pada parameter *P, Km* dan dapat dikenali dalam himpunan $ID \in \{0,1\}$ dan memiliki kunci private pada *d* untuk pengguna *ID*,

3. Ketika melakukan enkripsi pada parameter *P*, pesan $m \in M$ dan $ID \in \{0,1\}^*$ mendapatkan keluaran berupa enkripsi $c \in C$
4. Dan ketika melakukan dekripsi nya maka jalur protocol *d* dilewati. *P* dan $c \in C$ dibalikan dengan membuka pesan $m \in M$.

Ini yang terjadi pada algoritma IDE, dapat kita lihat bahwa algoritma ini yang bila dikombinasikan dengan algoritma RSA akan memberikan pengamanan yang sudah cukup baik, tetapi di dalam algoritma ini hanya mengandalkan jalur pada protocol *d* saja, akibatnya jika jalur dan protocol tersebut sudah diketahui maka setiap aktifitas yang melewati protokol tersebut akan mudah untuk dilacak walaupun algoritma RSA masih mengamankannya tanpa memberikan kunci private nya, akan lebih baik jika algoritma ini tidak hanya mengandalkan jalur ataupun protocol terstentu saja, namun dengan bantuan fuzzy logic dapat mengetahui setiap orang yang berhak mengambil dokumen atau file tersebut.

2 Metode Penelitian

Pada penelitian ini, menggunakan simulasi untuk menggambarkan ketika kedua algoritma tersebut bekerja di dalam jaringan dengan Riverbed Modeler untuk menjelaskan simulasi yang ada sehingga dapat dilihat apakah serangan phising itu dapat terjadi atau tidak pada kombinasi model yang digunakan, proses penelitian ini menggunakan skema seperti berikut :



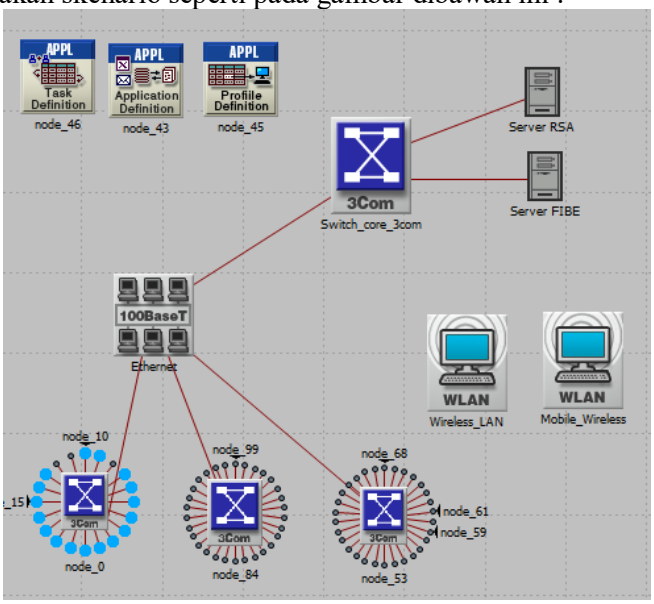
Gambar 1. Desain Skenario Kombinasi Algoritma

Pada proses di gambar 1. dapat terlihat metode dan proses untuk pengiriman data, dokumen ataupun file yang diamankan dengan menggunakan kombinasi dari Algoritma RSA dan FIBE, proses pertama diawali dengan Person A mau mengirim suatu dokumen atau file kepada Person B, maka dokumen tersebut akan di kirimkan melalui Cloud ataupun Internet, dimana dokumen tersebut sampai di router akan dilarikan dahulu oleh agent yang ada di PC, Laptop ataupun smartphone ke Generator Server untuk menempelkan kunci publik yang nantinya kunci public tersebut akan diterima oleh Person B, sewaktu diterima oleh Person B, *Internet Protocol (IP),* dalam bentuk email maupun attachment email, agent atau perangkat lunak yang diinstalkan ke dalam Client yang menggunakan protokol *User Datagram Protocol (UDP)* untuk mengkomunikasikan dengan Server Generator setiap informasi yang ada di Client atau penerima dalam hal ini Person B, yang akan melakukan pengecekan terlebih dahulu kepada Server Generator, dengan menggunakan Fuzzy Identity Based, setiap hal yang diperlukan seperti alamat IP yang sering digunakan oleh Person B, baik itu alamat IP yang ada di PC atau internal IP maupun yang ada di router atau IP Publiknya, dilakukan juga pengecekan terhadap E-mail yang digunakan oleh Person B dengan tepat, dilakukan juga pengecekan terhadap sistem operasi yang biasa digunakan oleh Person B, misalkan Person B ternyata sering menggunakan Sistem Operasi Microsoft Windows 7 atau Macintosh, agent akan melaporkannya kepada server, dilakukan juga pengecekan terhadap E-mail client yang digunakan, misalkan Person B terbiasa menggunakan microsoft outlook atau langsung dari browser, dan yang lainnya, jika kebiasaan-kebiasaan tersebut sudah terekam dengan algoritma *Fuzzy Identity Based*, maka FIBE akan mengirimkan sinyal melalui agent untuk meminta dikirimkan kunci private nya, jika kebiasaan-kebiasaan yang dilakukan oleh penerima sudah cocok dengan kebiasaan yang terekam oleh database, agar enkripsinya dapat dibuka dan dokumen atau file tersebut dapat dibaca oleh Person B, jika terdapat penerima baru yang belum memiliki kebiasaan jika berbeda alamat email maka agent akan langsung meminta kunci private kepada Server Generator, dan merekam informasi pertama dari client tersebut adalah kebiasaan pertama, jika terdapat hal-hal diluar kebiasaan maka server generator akan langsung mengirimkan email kepada alamat email penerima tersebut untuk meminta konfirmasi, jika sudah di dapatkan konfirmasi maka email akan dikirimkan oleh server

generator kepada pengirim, jika memang orang tersebut melakukan hal-hal diluar kebiasaanya dan sudah dikonfirmasi oleh kedua pihak maka agent akan segera meminta kunci private kepada Server Generator untuk segera mengirimkan kunci privatenya, kedua algoritma baik itu RSA dan FIBE akan melakukan kombinasi sesuai dengan fungsinya masing-masing untuk mengamankan dokumen atau file yang dikirim tersebut, yang tentunya dibantu oleh Server Generator maupun agent yang di install di dalam PC, Laptop maupun Smartphone.

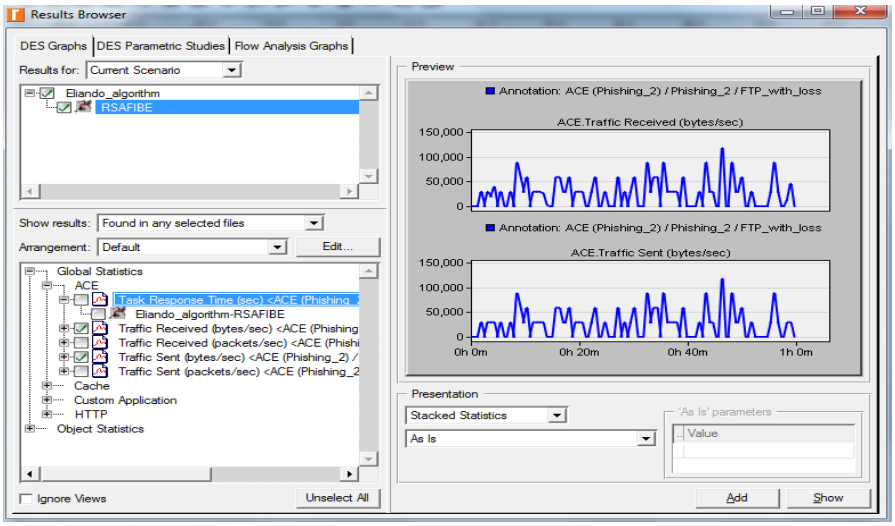
3. HASIL DAN PEMBAHASAN

Percobaan dilakukan dengan melakukan simulasi menggunakan Riverbed Modeler Academic Version yang menggunakan skenario seperti pada gambar dibawah ini :

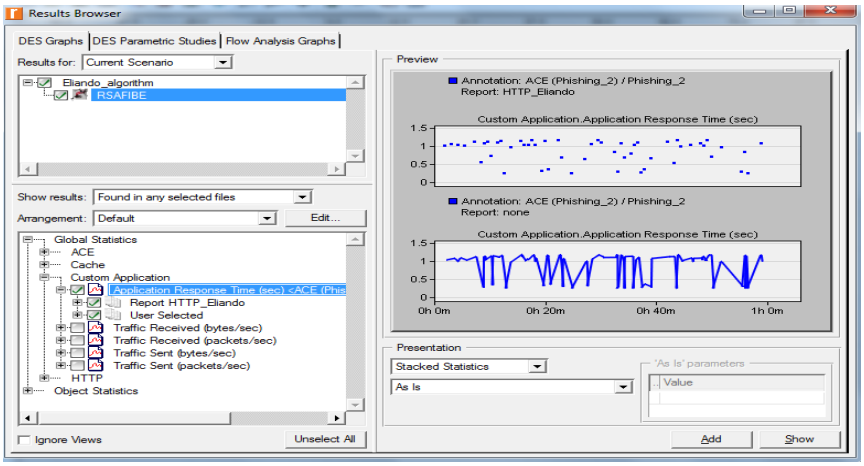


Gambar 2. Simulasi Algoritma RSA dan FIBE

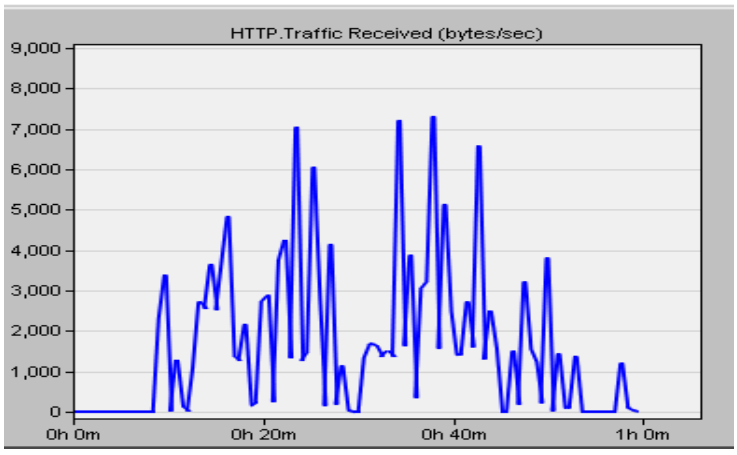
Pada Gambar 2. Terlihat ada sebuah kondisi jaringan yang memiliki banyak node serta workstation, yang terhubung dengan jaringan local, dan di setiap workstation dipasang aplikasi untuk melakukan scanner pada E-mail, lalu dijalankan tanpa henti untuk melakukan scanner E-mail di dalam jaringan, diujung jaringan local terdapat email server linux yang di proteksi dengan algoritma RSA dan Algoritma Fuzzy Identity Based, setelah itu dilakukan *Discrete Event Simulation* untuk menjalankan simulasi yang dijalankan yang menghasilkan ilustrasi berupa grafik seperti gambar dibawah ini :



Gambar 3. RSA Server Protection Response Graphic



Gambar 4. Phishing Attack Simulation Graphic



Gambar 5. HTTP FIBE Algorithm Response Graphic

Pada Gambar 5 dapat terlihat bahwa *HTTP Traffice Received* di drop sehingga menunjukan port 80 atau 8080 untuk port HTTP dapat tertembus oleh *scanner phishing* pada server dengan algoritma RSA dan pada Gambar 3, dapat terlihat bahwa server berusaha menekan serangan spear phishing dengan metode scanner E-mail, dan akhirnya melakukan *drop* terhadap *traffic* dari aplikasi tersebut pada algoritma FIBE, hal ini berbanding terbalik dengan pada Gambar 4. Dapat terlihat bahwa aplikasi terus berusaha melakukan scanner secara terus menerus karena memang diprogram demikian, dan ternyata dari simulasi ini terlihat bahwa *Spear Phishing* dengan metode email scanner tersebut dapat di *Drop* dengan kedua algoritma RSA dan *Fuzzy Identity Based* karena pada dasarnya scanner E-mail ketika berusaha untuk melihat isi server yang sudah memiliki kunci public dan kunci private dengan dikombinasi dengan enkripsi dari *Fuzzy Identity Based* sudah membuat sangat sulit untuk dibaca hasil E-mailnya, termasuk dengan cara simulasi sederhana ini, dengan menggunakan aplikasi yang dibuat sendiri, hingga saat ini Algoritma RSA masih merupakan algoritma yang terbaik, dengan terus merubah panjangnya kunci yang dimilikinya, sampai dengan saat ini jika tidak diketahui pola panjang kunci yang dimilikinya maka algoritma ini sudah cukup untuk dapat melindungi pesan atau file yang akan dikirim namun dengan kombinasi dari *Fuzzy Identity Based* maka tingkat kesulitan untuk melakukan dekripsi akan menjadi sangat sulit, karena FIBE selalu mempelajari akan pengguna yang berhak memiliki kunci untuk melakukan dekripsi terhadap pesan atau file yang dikirimkan, sehingga dapat dibuatkan sebuah formula kombinasi seperti dibawah ini :

$$S = \sum_{k=1}^{n}(Ph)k - \sum_{k=0}^{n}\binom{n}{k}RSA^{k}FIBE^{k} \quad \textbf{(1)}$$

Formula diatas memiliki penjelasan sebagai berikut
S = Secure Server
Ph = Phishing
n = Banyaknya komputer atau client atau web atau aplikasi E-mail
k = Konstanta pembentuk
Formula ini dapat dikembangkan nantinya untuk mencari *Positive Spear Phishing* untuk menguji kembali setiap komputer yang benar-benar berhasil diserang dan kondisi dari algoritma RSA dan algoritma FIBE setelah mengalami beberapa tahap pengujian, dari formula ini nanti akan diketahui lebih dalam apakah kedua algoritma ini dapat disatukan, pada penelitian saat ini kedua algoritma ini berdiri sendiri-sendiri pada masing-masing server dan kedua nya memiliki karakteristik yang berbeda, yang memiliki satu kesamaan yaitu melindung data atau informasi yang ada di dalamnya sehingga dari hasil simulasi diatas *Spear Phishing* tidak berhasil dilakukan pada masing-masing algoritma, atau dapat disimpulkan kedalam dalam tabel berikut :

Table 1. Perbandingan *Phishing Tools Attack*

	SERVER		
Phishing Attack	RSA	Fuzzy Identity Based Encryption (FIBE)	RSA+ FIBE
Phishing tools attack with E-mail Scanner	Not Succeed	Not Succeed	Not Succeed
Phishing tools attack to HTTP	Succeed	Not Succeed	Not Succeed

4. KESIMPULAN

Spear Phishing merupakan bentuk serangan yang terus menerus untuk mencari korban untuk mencuri data atau informasi apapun, sehingga hal ini menjadi sangat berbahaya apabila informasi tersebut disalahgunakan. Algoritma RSA dan FIBE merupakan algoritma yang tepat untuk melindungi dari serangan spear phishing, yang masih harus diteliti lebih lagi, mengenai kombinasi kedua nya. Penelitian ini masih merupakan dasar dari kekuatiran akan dapat diretasnya algoritma RSA yang mengakibatkan *Spear Phishing* dapat dilakukan, karena bukan tidak mungkin hal yang dibuat manusia tidak dapat diretas, jika hal itu terjadi *Fuzzy Identity Based Encryption* (FIBE) merupakan algoritma yang tepat untuk dapat dikembangkan bersama algoritma RSA untuk dapat semakin melindungi data ataupun informasi penting yang ada di dalamnya.

Daftar Pustaka

1. Amin, Mukhlis: Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (Mcda). Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika, Vol. 5 No. 1 (2014).
2. Rachmawati, Dian: Jurnal SAINTIKOM Vol. 13, No.3 (2014).
3. Ginting, Albert., Isnanto, R. Rizal., Windasari, I. Pertiwi: Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email, Jurnal Teknologi dan Sistem Komputer, Vol.3, No.2 (2015).
4. Anwar, Nuril., Riadi,Imam., Luthfi, Ahmad: Analisis SIM Card Cloning Terhadap Algoritma Random Number Generator, Jurnal Buana Informatika, Volume 7, No 2, (2016) 143-150.
5. Anggorojati, Bayu., Prasad, R: Securing Communication In The IOT-Based Health Care Systems, Jurnal Ilmu Komputer dan Informasi (Journal of a Science and Information). 11/1 (2018), 1-9.
6. Mansur,Khairunnisa., Hasanuddin. B,Zulfajri., Wardi: Sistem Keamanan Informasi pada Smart Gate Menggunakan Visual Basic, Jurnal Penelitian Enjiniring, Fakultas Teknik, Universitas Hasanuddin (2017).
7. Jun-Ho Huh, Seung-Mo Je, Kyungryong Seo: Design and Configuration of Avoidance Technique for Worst Situation in Zigbee Communications Using OPNET, Information Science and Applications (ICISA) (2016) pp 331-336.
8. Yi jun Mao, Jin Li, Min-Rong Chen, Jianan Liu e, Congge Xie e, Yiju Zhan: Fully secure fuzzy identity-based encryption for secure IoT communications, Computer Standards & Interfaces 44, Elsevier B.V. (2016) 117–121,
9. Tout, Hicham., Hafner, William: Phishpin: An Identity-Based Anti-Phishing Approach, International Conference on Computational Science and Engineering, IEEE (2009).
10. Zhao, Mengchen., An, Bo., Kiekintveld, Christopher: Optimizing Personalized Email Filtering Thresholds to Mitigate Sequential Spear Phishing Attacks, Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence (2016).