ISSN 2085-4552

Implementasi Zero Knowledge Proof Menggunakan Protokol Feige Fiat Shamir Untuk Verifikasi Tiket Rahasia

Willy Sudiarto Raharjo, Dessy Sutanti
Program Studi Teknik Informatika, Universitas Kristen DW Yogyakarta, Indonesia
willysr@ti.ukdw.ac.id, dessy.sutanti@ti.ukdw.ac.id

Diterima 10 September 2015
Disetujui 9 Oktober 2015

Abstract— **Cryptography is known for it's ability to protect confidential information, but it can also be used for other purposes. One of them is for identity verification or authentication. One of the biggest disadvantages of traditional authencation method is at the end of the session, the verifier knows about secrets which is supposed to be known only by prover. In this paper, we implemented a Zero-Knowledge Proof-based secret ticket verification system using Feige Fiat Shamir protocol. The goal of this system is to help prover identified themselves to the verifier, but also prevent the verifier to understand anything about the prover's secret information. The system is also able to prevent ticket duplication or double-use of tickets by using an interactive proof verification method. By combining it with cryptography, not only we can achieve completeness and soundness property of Zero-Knowledge Proof, but we can also achieve information security property.**

Index Terms— Feige-Fiat Shamir, Verification, Zero Knowledge Proof

I. Pendahuluan

Dalam pengiriman informasi dengan beberapa teknik kriptografi, dibutuhkan suatu cara agar informasi yang ingin disampaikan dapat diterima dengan aman oleh pihak yang berwenang mendapatkannya. Saat seseorang menerima atau mengirimkan pesan, terdapat tiga persoalan yang sangat penting, yaitu *confidentiality* (menjamin data tidak dapat dibaca oleh orang yang tidak berkepentingan), *authenticity* (menjamin keaslian data serta dengan siapa komunikasi dilakukan), dan *integrity* (menjamin data yang dikirim sama dengan data yang diterima) [1]. Ketiga hal ini merupakan prinsip dasar dari keamanan informasi yang sering juga disebut dengan CIA.

Salah satu bentuk proses pengiriman informasi yang membutuhkan pengamanan adalah tiket. Tiket yang dimaksud merupakan sebuah kunci utama untuk mendapatkan akses masuk yang hanya diketahui oleh pihak berwenang. Namun terdapat beberapa resiko kecurangan yang dapat dilakukan pihak lain seperti membuat tiket palsu dan penggandaan tiket. Dalam proses verifikasi sebuah tiket, sangat penting untuk memastikan bahwa pihak lain yang tidak memiliki hak tidak akan mendapatkan informasi apapun pada saat proses verifikasi sedang berlangsung maupun setelah proses selesai. Namun demikian, proses verifikasi akan tetap dilakukan dengan informasi yang tersedia.

Untuk memenuhi kebutuhan akan keamanan verifikasi tiket, maka digunakan salah satu teknik kriptografi yaitu *Zero Knowledge Proof* (ZKP) yang memberikan kemampuan kepada seorang *prover* untuk membuktikan bahwa dirinya memiliki suatu informasi rahasia tanpa memberitahukan isi dari informasi tersebut dan proses verifikasi menggunakan protokol Feige-Fiat Shamir. Di dalam penerapannya, terdapat tiga stakeholder yaitu *prover* (membuktikan kepemilikannya akan tiket rahasia), *verifier* (diasumsikan sebagai penjaga yang melakukan proses verifikasi), dan pihak ketiga (*arbiter*) yang menghasilkan dan mengatur proses pengiriman tiket dan tiket rahasia ke pihak *prover* dan *verifier*.

Tujuan dari penelitian ini adalah untuk menghasilkan sebuah sistem yang mampu melakukan proses verifikasi tiket serta mencegah

penyalahgunaan tiket, yaitu duplikasi maupun penggunaan tiket sebanyak dua kali atau lebih pada satu sesi yang sama dengan menggunakan implementasi *Zero Knowledge Proof* berbasis pada protokol Feige Fiat Shamir.

II. TINJAUAN PUSTAKA

Penerapan *Zero Knowledge Proof* tidak hanya terbatas pada pembuktian informasi rahasia, namun juga bisa digunakan pada model authentikasi. Quan, Mikhail, dan Arjun menggunakan *Zero Knowledge Proof* untuk membangun sebuah *Two-Factor Authentication system* berbasiskan protokol ZKP [2].

Thiruvaazhi dan Diyva mengembangkan sebuah protokol untuk proses authentikasi web menggunakan *Zero Knowledge Proof* untuk mengatasi permasalahan yang ditemukan ketika menggunakan *password-based client authentication* dan *PKI-based server authentication* [3].

Zero Knowledge Proof juga bisa digunakan untuk mekanisme pertukaran kunci pada perangkat mobile dengan menggunakan teknik *hashing* pada mobile RFID [4].

III. LANDASAN TEORI

A. Kriptografi

Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan [5]. Setiap keunikan menunjukkan bahwa cara menulis pesan rahasia mempunyai nilai estetika tersendiri sehingga kriptografi berkembang menjadi sebuah seni merahasiakan pesan (kata "graphy" di dalam "cryptography" itu sendiri sudah menyiratkan sebuah seni [6]). Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. Data sandi tersebut hanya dapat dikembalikan ke bentuk data sebenarnya dengan menggunakan kunci (*key*) tertentu yang dimiliki oleh pihak yang sah saja.

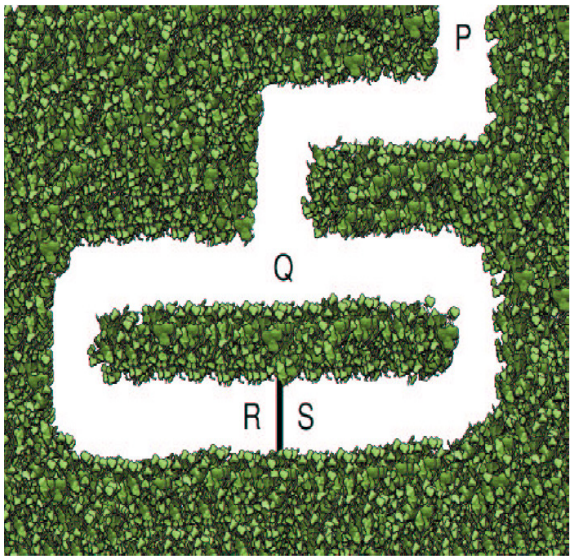
Dalam perkembangannya, kriptografi telah banyak dipakai di berbagai aplikasi, termasuk didalamnya email, perbankan, sertifikat digital, dan lain sebagainya. Hal ini menjadi salah satu alasan kenapa ilmu kriptografi berkembang semakin pesat seiring dengan semakin banyaknya implementasi dunia kriptografi di berbagai bidang. Perubahan ini menuntut bahwa dunia kriptografi tidak lagi hanya berdasarkan pada sebuah seni, namun didasarkan oleh pembuktian yang dilakukan secara formal.

Pada tahun 1985 diperkenalkan sebuah prosedur untuk pembuktikan teorema yang menyatakan bahwa "*proof*" bersifat probabilitas dan pada input sebanyak N-bit, kita bisa tidak mempercayai tingkat kebenarannya dengan nilai probabilitas yang sangat kecil, misalnya $\frac{1}{2^n}$ dan sangat yakin dengan tingkat kebenarannya dengan nilai probabilitas yang sangat tinggi, misalnya 1-$\frac{1}{2^n}$ [7]. Untuk bisa melakukan verifikasi kebenaran dari sebuah pernyataan secara efisien, maka "*recipient*" dari sebuah "*proof*" harus bertanya secara aktif dan menerima jawaban dari "*prover*".

B. Zero Knowledge Proof

Zero Knowledge Proof (ZKP) merupakan protokol kriptografi yang dapat digunakan seseorang untuk membuktikan kepemilikan seseorang (*prover*) akan suatu informasi rahasia kepada orang lain (*verifier*), tanpa perlu mengungkapkan informasi tersebut atau memberikan cara bagi orang lain untuk mengetahui rahasia tersebut. Hal ini sangat berguna sekali dalam implementasi pada dunia kriptografi, terutama pada pemanfaatan *public-key cryptography* dimana terdapat dua pihak yang ingin berkomunikasi dan pihak pertama dapat melakukan proses verifikasi terhadap identitas pihak kedua dengan memanfaatkan kunci publik yang dimiliki. Proses verifikasi dilakukan dengan menggunakan model *challenge-response*, baik yang bersifat interaktif maupun non-interaktif. Dengan menggunakan konsep ZKP, maka pihak pertama dapat merasa yakin bahwa pihak kedua merupakan orang yang sesuai dengan identitasnya dengan menggunakan sebatas informasi yang dapat diperoleh dari kunci publik. Selain itu, dari kunci publik yang dihasilkan pihak kedua dan sudah dimiliki oleh pihak pertama, tidak akan didapatkan informasi rahasia yang hanya diketahui oleh pihak kedua yaitu informasi yang tersimpan dalam kunci privatnya.

Salah satu contoh ilustrasi kasus dari penerapan ZKP yang terkenal adalah gua Alibaba seperti pada Gambar 1.



Gambar 1 Ilustrasi Gua Alibaba[8]

Gua tersebut memiliki sebuah pintu rahasia diantara jalur R dan S. Langkah-langkah pembuktiannya adalah sebagai berikut [9]:

1. *Verifier* berada pada posisi P, sedangkan *prover* berada di posisi Q.

2. *Prover* akan berjalan menuju ke pintu dengan menggunakan jalur R atau S sesuai dengan keinginan *prover* dan dilakukan secara acak.

3. Setelah itu *verifier* akan berjalan ke posisi Q dan meneriakkan jalur R atau S sesuai dengan keinginannya, kemudian *prover* berjalan ke arah posisi Q menggunakan jalur yang telah disebutkan oleh *verifier*.

4. Jika prover mengetahui kata rahasia untuk membuka pintu, maka *prover* akan mampu mengikuti semua permintaan *verifier*, tetapi jika *prover* ingin mengelabui *verifier*, maka *prover* memiliki probabilitas 50% untuk berhasil.

Protokol ZKP harus memenuhi 3 properti, yaitu *completeness*, *soundness*, dan *zero-knowledge* [9]. Properti completeness menyatakan apabila pernyataan bernilai benar, maka *verifier* yang jujur akan percaya dengan bukti-bukti yang diberikan oleh *prover* yang jujur. Properti *soundness* menyatakan apabila pernyataan bernilai salah, tidak ada *prover* curang yang bisa meyakinkan *verifier* yang jujur bahwa pernyataan itu benar, kecuali dengan tingkat probabilitas yang sangat kecil. Properti *Zero-Knowledge* menyatakan bahwa jika pernyataan bernilai benar, maka tidak ada *verifier* curang yang bisa mempelajari apapun selain fakta yang ada.

C. Feige-Fiat Shamir

Feige-Fiat Shamir merupakan salah satu protokol Zero Knowledge Proof yang sering diimplementasikan sebagai protokol pembuktian identitas (*identity proof*). Protokol ini secara umum bekerja dengan langkah-langkah sebagai berikut [10]:

1. Penghitungan awal : *Arbiter* menghasilkan bilangan acak modulus n (512-1024 bits) yang merupakan hasil perkalian dua bilangan prima yang besar

$$n = p * q \quad (1)$$

Arbiter menghasilkan sepasang kunci publik dan privat untuk *prover* dengan memilih angka V, yang merupakan sisa dari hasil pangkat dua modulus n .

$$V = S^2 \bmod n \quad (2)$$

V adalah kunci publik, sedangkan S adalah kunci privat dimana $S_1, \ldots, S_k$ dengan syarat gcd(S,n)=1 dimana gcd adalah *Greatest Common Divisor* atau Faktor Persekutuan Terbesar.

2. Proses identifikasi protokol : *Prover* mengambil angka *random* r dimana r < n. Kemudian *prover* akan menghitung nilai x dan mengirimkannya ke *verifier*.

$$x = r^2 \bmod n \quad (3)$$

3. *Verifier* memilih e ϵ {0,1} sepanjang k dan mengirimkannya kembali ke *prover*.

4. *Prover* mengirimkan nilai y:

$$y = r * S^e \bmod n \quad (4)$$

5. *Verifier* melakukan pembuktian

$$y^2 \equiv x * V^e \,(mod\ n) \quad (5)$$

6. Selesai

IV. IMPLEMENTASI SISTEM

Sesuai dengan protokol Feige-Fiat Shamir, proses pertama yang dilakukan adalah pembuatan tiket. Pembuatan tiket ini harus dilakukan oleh *arbiter* (pihak ketiga) yang dipercaya, artinya *arbiter* dapat menjamin keamanan tiket.

Berikut ini adalah algoritma pembuatan tiket :

1. Mulai

2. *Arbiter* membangkitkan bilangan *random* p dan q. Bilangan p dan q ϵ prima, p dan q ϵ integer positif

3. *Arbiter* menghitung

$$n = p * q \quad (6)$$

4. *Arbiter* menentukan himpunan S

$$S = < s_i \mid gcd\ (s_i, n = 1)\ ,\ 1 \leq i \leq n > \quad (7)$$

5. *Arbiter* menentukan himpunan V

$$V = < v_i \mid s_i^2 \bmod n = v,\ s_i \epsilon\ S > \quad (8)$$

6. *Arbiter* mengirimkan *output* tiket berisi V kepada *verifier* dan S, V kepada *prover*

7. Selesai

Setelah proses pembuatan tiket selesai, maka hal yang selanjutnya dilakukan adalah proses verifikasi tiket. Berikut ini adalah algoritma verifikasi tiket :

1. Mulai

2. *Verifier* menentukan himpunan bilangan *random* R

$$R = < r_i \mid r_i\ \epsilon\ integer\ positif\ ,\ 0 \leq i \leq t$$

$$t\ \epsilon\ integer\ positif > \quad (9)$$

3. Inisialiasi i = 0; i ≤ t, i++

4. *Prover* menentukan himpunan x (disebut acuan) kemudian dikirimkan ke *verifier*

$$A = < a_i \mid a_i = r_i^2 \bmod n,\ r_i \epsilon\ R > \quad (10)$$

5. *Verifier* menentukan himpunan E

$$E = < e_i \mid e_i \epsilon\ \{0,1\},\ 0 \leq i \leq |S| > \quad (11)$$

6. *Prover* menentukan himpunan Y untuk dikirimkan ke *verifier*

$$Y = < y_i \mid y_i = r_i * s_i^e \bmod n,\ r_i \epsilon\ R,$$

$$s_i \epsilon\ S,\ e_i \epsilon\ E > \quad (12)$$

7. *Verifier* menentukan himpunan Y*

$$Y^* = < y_i^* \mid y_i^* = a_i * v_{i\,i}^e \bmod n$$

$$a_i \epsilon\ A,\ v_i \epsilon\ V,\ e_i \epsilon\ E > \quad (13)$$

8. Jika $y^2 \equiv x * V^e \bmod n$ maka sistem memberikan *output* verifikasi berhasil

Jika $y^2 \equiv x * V^e \bmod n$ atau $y^2 = 0$ maka sistem memberikan *output* verifikasi gagal

9. Selesai

Pada penelitian ini tiket tidak divisualisasikan dalam bentuk fisik seperti halnya tiket pada umumnya, namun dinyatakan dalam bentuk angka-angka yang mencerminkan nilai pada hasil perhitungan pada pembuatan kunci publik dan privat.

Untuk meningkatkan keamanan sistem, maka pada waktu pembuatan tiket, juga dilengkapi dengan kata sandi yang dienkripsi menggunakan algoritma AES dengan kunci 256-bit untuk kunci privat.

V. PENGUJIAN SISTEM

Pengujian dilakukan dengan pembuatan 5 tiket oleh *arbiter*, kemudian dilanjutkan dengan proses verifikasi tiket. Pada proses verifikasi tiket ini akan terlihat hasil implementasi *Zero Knowledge Proof* serta keamanan dari protokol *Feige-Fiat Shamir.*

Gambar 2 merupakan antarmuka untuk proses pembuatan tiket, sedangkan Gambar 3 merupakan tampilan saat proses verifikasi tiket yang valid sedangkan Gambar 4 merupakan tampilan saat proses verifikasi tiket yang tidak valid. Tiket palsu dihasilkan dengan mengubah sebagian nilai file tiket dengan nilai yang *random*. Misalkan pada contoh di Gambar 3, baris 1 terdapat perubahan nilai dari angka 25 menjadi 30. Perubahan ini dilakukan pada posisi yang *random* untuk mensimulasikan hasil tiket yang benar-benar berbeda. Hasil pembuatan tiket secara *random* dapat dilihat pada Tabel 1.

Untuk pengujian, setiap tiket akan diujikan sebanyak 20 kali dengan nilai kunci yang dihasilkan secara *random* dan dikatakan proses verifikasi berhasil apabila pada semua pengujian kunci dapat diverifikasi dengan baik seperti pada langkah 8 pada proses verifikasi tiket. Apabila terdapat satu kegagalan pada proses pengujian, maka kunci akan dianggap tidak valid. Jumlah iterasi sebanyak 20 dirasa sudah memadai mengingat probabilitas *adversary* untuk menipu *verifier* sangatlah kecil. Hal ini disebabkan karena protokol Fiat-Shamir merupakan *three-pass protocol* yang berdasarkan pada kerumitan dalam melakukan proses faktorisasi dan sampai dengan hari ini masih dianggap sebagai sebuah *hard problem* [11].

Untuk menguji keamanan dari protokol ini sekaligus untuk mencegah terjadinya modifikasi terhadap tiket yang bisa berujung pada duplikasi atau penggunaan ganda tiket, maka pada pengujian berikutnya dilakukan modifikasi terhadap tiket dan hasilnya digunakan sebagai input untuk proses verifikasi tiket. Hasil pengujian untuk tiket yang valid ditunjukan pada Tabel 2 sedangkan untuk pengujian tiket yang tidak valid ditunjukan pada Tabel 3. Tiket yang sudah pernah dipakai akan disimpan didalam sistem sehingga tidak akan bisa digunakan untuk kedua kalinya.

Berdasarkan tabel tersebut, dapat diketahui bahwa proses verifikasi dengan tiket asli akan selalu diterima yang berarti *prover* berhasil membuktikan kepemilikannya akan tiket dan file kode rahasia kepada *verifier*. Sedangkan pada Tabel 3 dapat diketahui bahwa proses verifikasi untuk tiket palsu selalu ditolak (verifikasi gagal). Hal ini membuktikan bahwa tiket tidak dapat dipalsukan dengan mudah dan untuk bisa menipu *verifier*, maka tiket yang palsu harus bisa menjawab semua *challenge* yang diberikan oleh *verifier* dengan benar. Apabila terdapat satu kegagalan proses verifikasi pada salah satu percobaan saja, maka tiket akan dianggap palsu dan tidak bisa digunakan.

Tabel 1. Hasil Pembuatan Tiket

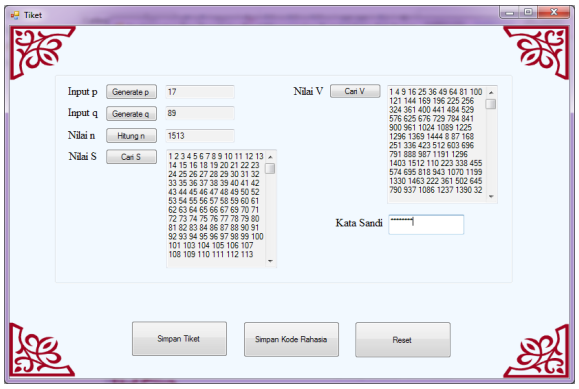
No.	Nilai p	Nilai q	Nilai n	Kata Sandi
1.	17	89	1513	71110020
2.	83	59	4897	dessy0020
3.	53	37	1961	d355y
4.	17	37	629	tiket1234
5.	31	79	2449	12juni

Tabel 2. Hasil Pengujian Tiket dengan Data Valid

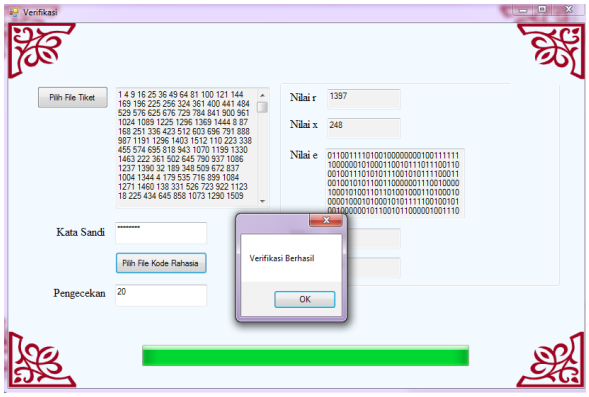
No.	Tiket	Jumlah Pengecekan	Status Verifikasi
1.	Tiket 1	20	Verifikasi Berhasil
2.	Tiket 2	20	Verifikasi Berhasil
3.	Tiket 3	20	Verifikasi Berhasil
4.	Tiket 4	20	Verifikasi Berhasil
5.	Tiket 5	20	Verifikasi Berhasil

Tabel 3. Hasil Pengujian Tiket dengan Data Palsu

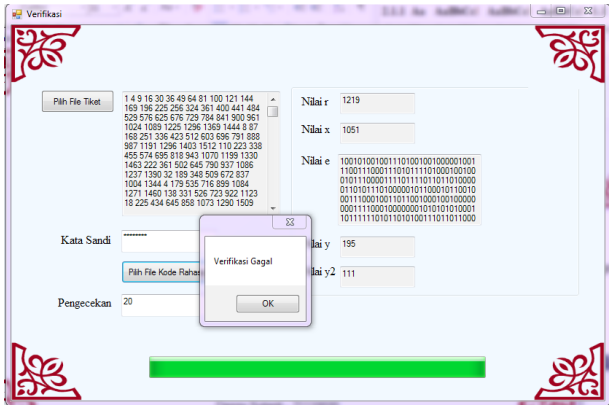
No.	Tiket	Jumlah Pengecekan	Status Verifikasi
1.	Tiket 1	20	Verifikasi Gagal
2.	Tiket 2	20	Verifikasi Gagal
3.	Tiket 3	20	Verifikasi Gagal
4.	Tiket 4	20	Verifikasi Gagal
5.	Tiket 5	20	Verifikasi Gagal



Gambar 2 Proses Generate Tiket



Gambar 3 Proses Verifikasi Tiket Valid



Gambar 4 Proses Verifikasi Tiket Tidak Valid

VI. KESIMPULAN

Berdasarkan hasil implementasi dan analisis yang telah dibuat dibahas pada bab sebelumnya, maka dapat disimpulkan sebagai berikut :

1. Proses verifikasi tiket menggunakan protokol *Feige-Fiat Shamir* dapat berjalan dengan baik dan aman. Salah satu keamanan proses verifikasi terdapat pada enkripsi file kode rahasia (representasi kunci privat). Sebelum memulai verifikasi, file kode rahasia harus didekripsi terlebih dahulu menggunakan kata sandi yang hanya diketahui oleh *prover*, sehingga kemungkinan untuk pemalsuan / penggandaan tiket oleh pihak tidak berwenang sangat kecil.

2. Pihak *verifier* tidak dapat mencurangi tiket rahasia, karena saat proses verifikasi sistem memerlukan kata sandi yang hanya diketahui oleh *prover*. Walaupun *verifier* memalsukan tiket, namun sistem tetap mengenali tiket tersebut sebagai tiket palsu, sehingga hasil yang dikeluarkan oleh sistem akan memberikan keputusan yang tepat (memberikan akses atau tidak). Keberhasilan sistem mengenali tiket palsu ini didapatkan melalui hasil penghitungan dengan protokol *Feige-Fiat Shamir*.

3. Tiket rahasia dan kata sandi menjadi kunci utama yang dimiliki oleh *prover* untuk melakukan verifikasi. Dengan kata lain jika ada pihak yang tidak memiliki tiket rahasia dan kata sandi namun mencoba untuk melakukan verifikasi, maka sistem akan mengidentifikasi pihak tersebut menggunakan tiket palsu.

4. Dalam proses verifikasi, *prover* selalu dapat membuktikan kepemilikannya terhadap tiket (*completeness*) dan apabila gagal verifikasi maka tidak akan mendapatkan akses masuk (*soundness*).

VII. SARAN

Beberapa saran yang dapat menjadi masukan untuk penelitian selanjutnya:

1. Visualisasi tiket yang lebih baik, misalnya dengan menggunakan QR code.

2. Pemanfaatan *two-factor authentication* untuk meningkatkan keamanan dari kunci privat.

3. Pemanfaatan algoritma ZKP yang lain sebagai pembanding, misalnya Schnoor.

4. Pemanfaaatan mekanisme *non-interactive Zero Knowledge Proof* .

5. Jumlah iterasi yang digunakan untuk proses pembuktian bisa ditentukan oleh verifier.

Daftar Pustaka

[1] Stamp, M., “Information Security: Principles and Practices”. Wiley, 2011.

[2] Nguyen Q., Rudoy, M., Srinivasan, A., “Two Factor Zero Knowledge Proof Authentication System”, 2014.

[3] Thiruvaazhi, U. and Divya, R.(2011) ‘Web Authentication Protocol Using Zero Knowledge

Proof',Information Security Journal: A Global Perspective, 20: 2, 112 — 121

[4] Kurmi, J., Sodhi, A., "A Survey of Zero-Knowledge Proof for Authentication", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 5, Issue 1, Januari 2015.

[5] Schneier, B. "Applied Cryptography : Protocols, Algorithms, and Source Code in C (2nd edition)", John Wiley & Sons,Inc., New Jersey, 1996.

[6] Mollin, R.A. "An Introduction to Cryptography (2nd edition)", Chapman & Hall/ CRC, Florida, 2006.

[7] Goldwasser, S., Micali, S., Rackoff, C., "The Knowledge Complexity of Interactive Proof-Systems", Proc. 17th *STOC,* 1985, pp. 291–304.

[8] Raffo, D., "Digital Certificates and the Feige-Fiat Shamir Zero Knowledge Protocol. France : Traineeship report, 2012.

[9] Situngkir, T.N., "Implementasi Zero Knowledge Proof dengan Feige Fiat Shamir dan Quadratic Linear Congruential Generator" (Skripsi), Ilmu Komputer, Universitas Sumatera Utara, Medan, Indonesia, 2013.

[10] Knapp, J, "Overview of Zero-Knowledge Protocols", 2009

[11] Franco, J., "Feige-Fiat-Shamir Zero Knowledge Proof", University of Cincinnati, Ohio, 2009