PEMANFAATAN *USERNAME* SEBAGAI *ID* PUBLIK PADA LAYANAN *BLACKBERRY MESSENGER*

Alfian Ilarizky[1], Dwi Indah Retnoningtyas[2]
[1]*Bidang Minat Teknik Rancang Bangun Peralatan Sandi, Sekolah Tinggi Sandi Negara, Bogor*
E-mail: alvcrypt@gmail.com

[2]*Bidang Minat Manajemen Persandian, Sekolah Tinggi Sandi Negara, Bogor*
E-mail: indah.kirei89@yahoo.com

ABSTRAK

Di era modern ini, teknologi informasi dan komunikasi berkembang semakin pesat. Perkembangan ini menuntut adanya kebutuhan akan sarana dan prasarana yang mudah, cepat, dan memiliki fleksibilitas tinggi. Salah satu kebutuhan yang dapat memenuhi tuntutan tersebut adalah dengan menggunakan layanan internet. Penggunaan layanan internet ini juga kian meningkat karena adanya kebutuhan pengguna agar dapat berkomunikasi di seluruh belahan dunia. BlackBerry merupakan salah satu perangkat untuk berkomunikasi yang sedang populer di kalangan masyarakat. Salah satu layanan yang paling digemari dari BlackBerry ini adalah layanan BlackBerry Messenger (BBM). Dengan adanya BBM, para pengguna BlackBerry dapat memanfaatkan layanan pesan instant dengan menggunakan internet secara real-time. Untuk menggunakan layanan BBM, pengguna harus mengetahui PIN BlackBerry dari pihak yang akan diajak berkomunikasi. Namun dengan adanya PIN tersebut, BBM hanya menyediakan layanan otentikasi perangkat, sedangkan untuk otentikasi pengguna tidak didukung. Hal ini mengakibatkan semua pihak yang tidak dikenal dan mengetahui PIN tersebut dapat melakukan permintaan untuk berkomunikasi.Untuk menyediakan layanan otentikasi pengguna, BBM dapat memanfaatkan username yang bersifat unik sebagai ID publik sebagai pengganti PIN. Username dari pengguna dapat disimpan dalam database server yang dapat diakses oleh pengguna BBM. Hal ini memungkinkan pengguna BBM dapat memastikan pihak yang melakukan permintaan untuk berkomunikasi dari database tersebut.

Kata kunci : *Username, ID* Publik, *BlackBerry Messenger*

1. PENDAHULUAN

Berkomunikasi satu sama lain merupakan salah satu sifat dasar manusia sejak ada di muka bumi ini. Bagi manusia, komunikasi berfungsi sebagai sarana untuk saling memahami satu sama lain. Cara manusia berkomunikasi dari zaman dahulu sampai sekarang mengalami perkembangan. Salah satu sarana komunikasi manusia adalah melalui tulisan. Sebuah tulisan berfungsi menyampaikan pesan kepada pembacanya. Pesan itu sendiri merupakan suatu informasi yang dapat dibaca dan dimengerti maknanya [1].

Dengan adanya perkembangan zaman dan majunya teknologi informasi, maka berkembang pula media komunikasi yang digunakan. Salah satu media komunikasi yang sedang naik daun akhir-akhir ini adalah *BlackBerry* (BB). BB mulai dikenal sejak sekitar dua tahun yang lalu, dimana situs-situs jejaring sosial sedang *booming*. BB memiliki keunggulan tersendiri dibanding dengan perangkat komunikasi yang lain, diantaranya yaitu memiliki kemampuan mengakses internet yang kencang dan stabil. Oleh karena itulah, BB juga menjadi incaran di Indonesia.

Namun, akibat dari permintaan yang tinggi inilah, beberapa oknum mencari celah dan ingin mencari keuntungan lebih. Akibatnya pemakai awamlah korbannya. BB tidak hanya saja perangkat yang memiliki konektivitas/internet yang hebat melainkan memiliki fitur yang unik yang tidak dimiliki oleh handset lain. *Handset* biasa pada umumnya memakai IMEI (GSM) atau ESN (CDMA) sebagai identitas diri yang pernah juga dirancang supaya bisa memiliki keamanan jika terjadi tindakan pencurian atau kelalaian. Namun, karena satu dan lain hal, sistem keamanan dengan pemblokiran akses melalui IMEI/ESN tidak berbuah dengan baik. RIM selaku pemilik hak dagang dan sistem BB telah merancang satu sistem yang dinamakan PIN. PIN disini bukan PIN untuk menyalakan HP atau sistem keamanan dari SIM *card*. PIN pada BB ini adalah sederetan alfanumerik yang unik yang berfungsi sebagai pengenal supaya apa yang dikirim bisa sampai dengan tepat. PIN ini digunakan oleh sesama pengguna BB untuk berkomunikasi melalui layanan *BlackBerry Messenger* (BBM).

PIN ini mengikat disetiap unit BB seperti halnya IMEI/ESN pada sistem biasa hanya saja PIN ini dipakai sebagai pengenal unik yang hanya ditemui di unit *BlackBerry* semacam *virtual account*. Sistem *Push Mail BlackBerry* ataupun konektivitas serta keamanannya ditandai dari PIN ini pula. Jika satu *handset* BB dilaporkan hilang/dicuri atau alasan lain, maka RIM akan mengeluarkan PIN tersebut dari *server*/sistem dan secara otomatis PIN tersebut tidak akan lagi dikenali dan tidak akan bisa dipakai lagi untuk berinternetan. Untuk PIN yang mengalami hal ini disebut *suspend*.

Karena semua sistem adalah karya manusia maka sistem tersebut juga bisa ditembus oleh manusia. "Kreativitas" baru yang sedang marak adalah melakukan *cloning* atau penggandaan PIN dimana satu PIN yang seyogyanya hanya boleh dipakai pada satu unit BB, maka digandakan ke beberapa unit sekaligus. Hal ini menyebabkan, BB yang telah *suspend* bisa aktif kembali. Namun, jika PIN tersebut terdeteksi oleh operator atau RIM sebagai PIN ganda maka mereka tidak akan sungkan untuk men-*suspend* PIN tersebut terlepas apakah ia pemilik resmi PIN tersebut atau bukan [2].

PIN yang telah digandakan ini tentu saja dapat digunakan oleh pihak-pihak yang tidak berhak agar dapat berkomunikasi dengan orang lain pula. Untuk mencegah adanya penyalahgunaan PIN tersebut, maka diperlukan suatu alternatif lain yang dapat digunakan sebagai suatu identitas khusus yang dapat dipublikasikan. Identitas ini digunakan untuk mengenali apakah pihak yang me-*request* layanan *Black Berry Messenger* benar-benar orang yang dikenal atau bukan. Identitas ini ditujukan agar penggunaan PIN ini tidak merugikan pengguna BB yang sesungguhnya.

2. KRIPTOGRAFI

Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Masalah keamanan sering kurang mendapat perhatian dari para perancang dan pengelola sistem informasi [1]. Untuk menangani masalah keamanan sistem informasi yang meliputi kerahasiaan, integritas data, otentikasi, dan penyangkalan dapat diselesaikan dengan menggunakan kriptografi. Kriptografi tidak hanya menyediakan alat untuk keamanan pesan, tetapi juga sekumpulan teknik yang berguna. Kriptografi (*cryptography*) berasal dari Bahasa Yunani: "*cryptós*" artinya "*secret*" (rahasia), sedangkan "*gráphein*" artinya "*writing*" (tulisan). Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia) [3].

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita (Bruce Schneier - *Applied Cryptography*). Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, keabsahan data, integritas data, serta autentikasi data (A. Menezes, P. van Oorschot and S. Vanstone - *Handbook of Applied Cryptography*) [4].

2.1. Ancaman Keamanan

Terjadi banyak pertukaran informasi setiap detiknya di internet. Juga banyak terjadi pencurian atas informasi oleh pihak-pihak yang tidak bertanggungjawab. Ancaman keamanan yang terjadi terhadap informasi adalah [1]:

a. ***Interruption*** merupakan ancaman terhadap *availability* informasi, data yang ada dalam sistem computer dirusak atau dihapus sehingga jika data atau informasi tersebut dibutuhkan maka pemiliknya akan mengalami kesulitan untuk mengaksesnya, bahkan mungkin informasi itu hilang.
b. ***Interception*** merupakan ancaman terhadap kerahasiaan (*secrecy*). Informasi disadap sehingga orang yang tidak berhak dapat mengakses computer dimana informasi tersebut disimpan.
c. ***Modification*** merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan kemudian mengubahnya sesuai keinginan orang tersebut.
d. ***Fabrication*** merupakan anacaman terhadap integritas. Orang yang tidak berhak berhasil meniru atau memasulkan informasi sehingga orang yang menerima informasi tersebut menyangka bahwa informasi tersebut berasal dari orang yang dikehendaki oleh si penerima kembali.

2.2. Tujuan Kriptografi

Kriptografi bertujuan untuk memberi layanan keamanan (yang juga dinamakan sebagai aspek-aspek keamanan) sebagai berikut [3]:

a. **Kerahasiaan** (*confidentiality*), adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
b. **Integritas data** (*data integrity*), adalah layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. Dengan kata lain, aspek keamanan ini dapat

diungkapkan sebagai pertanyaan: "Apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi)?".

c. **Otentikasi** (*authentication*), adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diotentikasi asalnya. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan: "Apakah pesan yang diterima benar-benar berasal dari pengirim yang benar?".

d. **Nirpenyangkalan** (*non-repudiation*), adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan. Sebagai contoh misalkan pengirim pesan memberi otoritas kepada penerima pesan untuk melakukan pembelian, namun kemudian ia menyangkal telah memberikan otoritas tersebut.

3. PROTOKOL KRIPTOGRAFI

Secara umum protokol ialah aturan yang berisi rangkaian langkah-langkah, yang melibatkan dua atau lebih orang, yang dibuat untuk menyelesaikan suatu kegiatan. Dalam lingkup yang lebih sempit, protokol kriptografi diartikan sebagai protokol yang menggunakan kriptografi. Orang yang berpartisipasi dalam protokol kriptografi memerlukan protokol tersebut misalnya untuk berbagi komponen rahasia untuk menghitung sebuah nilai, membangkitkan rangkaian bilangan acak, meyakinkan identitas orang lainnya (otentikasi), dan berbagai penggunaan yang lain. Protokol kriptografi dapat dibangun dengan melibatkan beberapa algoritma kriptografi. [5]

4. *BLACKBERRY*

BlackBerry adalah perangkat seluler yang memiliki kemampuan layanan *push email*, telepon, dan sms. Menjelajah Internet, dan berbagai kemampuan nirkabel lainnya. Penggunaan *gadget* canggih ini begitu fenomenal belakangan ini, sampai menjadi suatu kebutuhan untuk *fashion*. BlackBerry pertama kali diperkenalkan pada tahun 1997 oleh perusahaan Kanada, *Research in Motion* (RIM). Kemampuannya menyampaikan informasi melalui jaringan data nirkabel dari layanan perusahaan telepon genggam hingga mengejutkan dunia [6].

4.1. Layanan *BlackBerry*

RIM telah menyediakan beberapa layanan khusus untuk *BlackBerry* yang memiliki multitasking, yaitu *BlackBerry Enterprise Server, BlackBerry Professional Software,* dan *BlackBerry Internet Service*. Untuk pribadi biasanya menggunakan layanan *BlackBerry Internet Service* (BIS) karena harganya terjangkau [6].

4.1.1. *BlackBerry Enterprise Server* (BES)

Salah satu kelebihan dari perangkat genggam *BlackBerry* yaitu terintegrasinya dengan layanan email, semuanya terorganisasi melalui perangkat *BlackBerry Enterprise Server* (BES). Layanan dari BES memungkinkan terintegrasinya jaringan email dari *Microsoft Exchange, Lotus Domino,* dan *Novell Group Wise*.

BES memang ditujukan bagi pelanggan korporasi dengan cakupan usaha yang besar. Perangkat lunak ini mengintegrasikan seluruh *smartphone BlackBerry* pada suatu organisasi dengan system perusahaan yang telah ada. Keuntungan yang diperoleh adalah memperluas komunikasi nirkabel dan data perusahaan kepada pengguna aktif dengan cara yang aman.

4.1.2. *BlackBerry Professional Software* (BPS)

BPS merupakan komunikasi nirkabel dan kolaborasi solusi bagi usaha kecil dan menengah. Menghadirkan berbagai fitur yang dibutuhkan karyawan dalam paket yang mudah dipasang dan harga yang lebih murah.

4.1.3. *BlackBerry Internet Service* (BIS)

Perangkat lunak yang diperuntukkan bagi pengguna pribadi ini memngkinkan pengguna mengintegrasikan *smartphone* dengan 10 akun email yang berbasis *Post Office Protocol* (POP3) dan *Internet Message Access Protocol* (IMAP). Menerima dan mengirim pesan instan, serta berselancar di internet. Dengan BIS, pengguna juga dapat membuka tambahan data (*attachment*) dalam bentuk *Excel, Word, Powerpoint,* pdf, zip, jpg, dan gif dengan tingkat kompresi data yang tinggi.

4.2. *BlackBerry Messenger*

Salah satu keunggulan *BlackBerry* adalah terdapatnya fitur *BlackBerry Messenger* (BBM). BBM adalah program pengirim pesan instan yang disediakan untuk para pengguna perangkat *BlackBerry*. Aplikasi ini mengadopsi kemampuan fitur atau aktivitas yang populer di kalangan pengguna perangkat telepon genggam. BBM merupakan salah satu keunggulan dari penggunaan perangkat *BlackBerry* selain layanan *Push Mail*. Layanan *Messenger* ini dibuat khusus bagi pemilik *BlackBerry* dan dirancang khusus untuk berkomunikasi di antara pengguna. Cara menggunakan BBM adalah dengan penghubung nomor PIN yang juga eksklusif dimiliki masing-masing perangkat *BlackBerry* [5].

Sebelum pengguna bisa *chat,* tentu saja harus me-*request* atau meminta PIN dari teman yang ingin diajak *chat*. Pada umumnya, BBM sudah terintegrasi dengan *handheld BlackBerry*. Namun, jika belum bisa men-*download*-nya melalui situs *BlackBerry* [7].

5. Rancangan Protokol

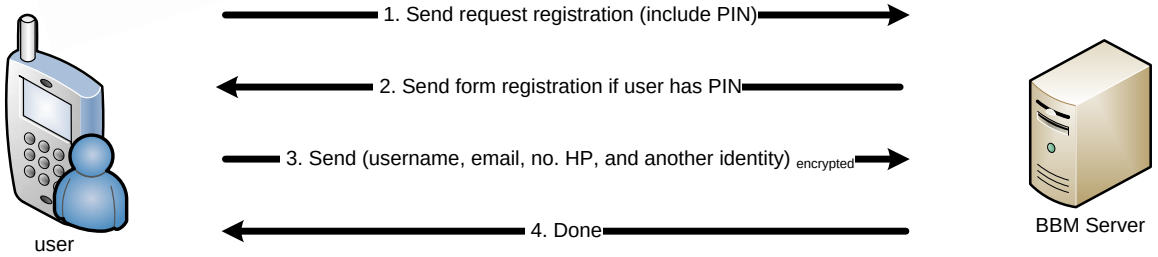
Protokol dari BBM merupakan protokol yang bersifat *propertiery* [8]. Protokol ini bersifat *propertiery* karena protokol ini merupakan protokol yang didesain oleh pihak pengembang *BlackBerry* (RIM) tanpa diumumkan kepada publik. Pihak RIM merahasiakan protokol yang digunakan meskipun RIM menyatakan bahwa penggunaan BlackBerry sudah cukup aman. Protokol BBM bekerja pada *transport layer* untuk mengirimkan pesan komunikasi. Untuk proses routing dan queueing dijalankan oleh infrastruktur dari RIM. Dalam proses kirim terima pesan, *server* khusus juga digunakan. *Server* BBM digunakan untuk menangani beberapa fungsi dari BBM, misalnya *BBM contacts remote (server) backup/restore, avatar supports, message multicast* [8].

Dalam perancangan protokol ini penulis mengabaikan protokol yang bekerja dalam infrastruktur RIM. Perancangan protokol ini dibuat untuk dipadukan dengan protokol dari BBM yang sudah dikembangkan oleh RIM sendiri. Segala aspek keamanan yang telah bekerja pada protokol asli dari BBM akan dipadukan dengan protokol kriptografi hasil modifikasi.

Protokol ini didesain untuk menanggulangi permasalahan penggandaan (kloning) PIN yang menjadi permasalahan dari *BlackBerry*. Penggunaan identitas publik yang bersifat unik dapat dimanfaatkan untuk mencegah terjadinya penggandaan PIN. Selain itu, identitas publik dapat dijadikan alat untuk identifikasi identitas dari pihak yang melakukan permintaan komunikasi.

Dalam perancangan protokol ini, pemanfaatan dari *server* BBM diperlukan untuk menyimpan identitas publik dari pengguna layanan BBM. Identitas publik yang digunakan dalam perancangan protokol ini memanfaatkan *username* yang telah terdaftar dalam *server* BBM. *Username* dalam *server* ini, terintegrasi dengan identitas pengguna yang lain seperti email, nomor HP, alamat rumah, tanggal lahir, dan bahkan foto profil dari pengguna.

Dalam protokol modifikasi ini, terbagi menjadi tiga tahap yaitu regsitrasi, pembuktian identitas, dan komunikasi. Tahap registrasi merupakan tahap awal dimana pengguna belum pernah melakukan komunikasi dengan memanfaatkan layanan BBM. Dalam tahap registrasi, PIN yang biasa melekat pada setiap *device* dari *BlackBerry* akan digunakan untuk validasi bahwa *device* yang digunakan merupakan *device* dari *BlackBerry*. Hal ini dapat mengurangi resiko dari penggandaan dari PIN *BlackBerry* karena PIN *BlackBerry* yang tersimpan pada *device* tidak harus bersifat unik. Langkah-langkah dari tahap registrsai terdapat pada gambar 1.



Gambar 1. Tahap registrasi

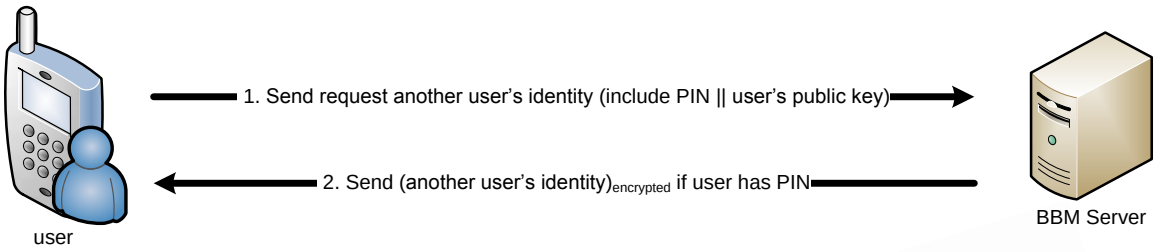
Penjelasan :

1. Pengguna akan mengirimkan permintaan untuk melakukan registrasi pada *server*. Dalam permintaan (*request)* tersebut, PIN dari *BlackBerry* akan ikut serta dikirim bersama permintaan registrasi.
2. *Server* akan memvalidasi PIN *BlackBerry* yang dikirim. Jika *device* dinyatakan benar memiliki PIN yang terdaftar pada *server*, maka *server* akan mengirimkan formulir registrasi pada pengguna.
3. Pengguna akan mengisi data diri pada formulir registrasi. Data diri tersebut merupakan identitas publik yang akan dikirim dan disimpan pada *database* dari *server* BBM. Data diri tersebut dikirim dengan

menggunakan enkripsi kunci publik. Kunci publik yang digunakan untuk enkripsi merupakan kunci publik dari *server*.

4.*Server* BBM akan mendekripsi data yang diterima kemudian menyimpan identitas tersebut. Proses registrasi selesai.

Tahap kedua dari protokol ini adalah tahap pembuktian identitas. Tahap ini bersifat *optional*, artinya tahap ini dapat dilakukan atau tidak. Pada tahap ini, pengguna dapat membuktikan kebenaran identitas dari pihak yang melakukan permintaan untuk komunikasi. Pengguna dapat memeriksa identitas pihak tersebut dengan mengakses identitas pihak tersebut melalui *server* BBM. Langkah-langkah dari tahap pembuktian identitas terdapat pada gambar 2.



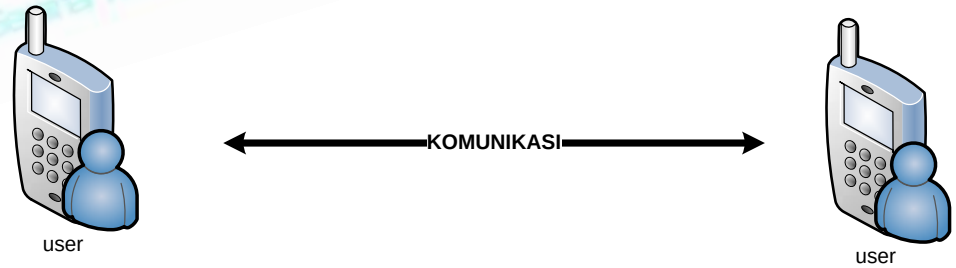
Gambar 2. Tahap pembuktian identitas

Penjelasan :

1.Pengguna akan mengirimkan permintaan identitas dari pengguna yang melakukan permintaan untuk komunikasi kepada *server*. Permintaan tersebut juga berisi PIN dan kunci publik dari pengguna.

2.*Server* akan memvalidasi PIN *BlackBerry* yang dikirim. Jika *device* dinyatakan benar memiliki PIN yang terdaftar pada *server*, maka *server* akan mengirimkan identitas dari pengguan yang melakukan permintaan untuk komunikasi. Identitas tersebut dikirim dengan melalui proses enkripsi menggunkan kunci publik dari pengguna. Pengguna dapat melihat identitas dari pengguna lain yang melakukan permintaan komunikasi setelah mendekripsi dengan menggunakan kunci privatnya. Setelah memeriksa identitas tersebut, pengguna dapat menentukan perlakuan terhadap pengguna tersebut. Perlakukan tersebut antara lain menerima (*accept*), menolak (*reject*), atau memblok (*block*) pengguna tersebut dalam melakukan layanan komunikasi BBM. Hal ini dapat memenuhi prinsip otentikasi pengguna dalam melakukan layanan BBM.

Tahap ketiga dari protokol ini adalah tahap komunikasi. Tahap ini merupakan bagian asli dari protokol komunikasi yang dikembangkan oleh pihak RIM. Proses kirim-terima pesan instan tetap menggunakan protokol BBM yang asli. Gambaran umum dari proses komunikasi antara pengguna ke pengguna terdapat pada gambar 3.



Gambar 3. Gambaran umum komunikasi pengguna ke pengguna.

6. KESIMPULAN

BBM merupakan layanan komunikasi pesan instan dari *BlackBerry* yang digemari oleh masyarakat. Layanan ini memliki beberapa kelemahan antara lain penggandaan (kloning) PIN dari *device BlackBerry* dan tidak adanya otentikasi pengguna. Solusi dari permasalahan ini antara lain dengan pemanfaatan *username* sebagai ID publik pada layanan BBM. *Username* ini bersifat unik dan mewakili data identitas yang lain dari pengguna. Data identitas tersebut antara lain email, nomor HP, alamat rumah, tanggal lahir, dan bahkan foto profil dari pengguna. *Username* yang tersimpan pada *server* BBM dapat mencegah dampak dari penggandaan PIN *BlackBerry*.

Keuntungan lain dari pemanfaatan *username* dalam protokol ini adalah terpenuhinya layanan otentikasi pengguna. Setiap pengguna dapat memeriksa identitas dari pengguna lain yang melakukan permintaan komunikasi dengan mengakses data identitas dari *server* BBM. Setelah memeriksa identitas tersebut, pengguna dapat menentukan perlakuan terhadap pengguna tersebut. Perlakukan tersebut antara lain menerima (accept), menolak (reject), atau memblok (block) pengguna tersebut dalam melakukan layanan komunikasi BBM. Hal ini dapat memenuhi prinsip otentikasi pengguna dalam melakukan layanan BBM.

DAFTAR PUSTAKA

[1]. Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi: Teori Analisis dan Implementasi.* Yogyakarta: Penerbit ANDI.

[2]. Kaskus: *The Largest Indonesian Community*. 2011. *"Serba-Serbi PIN Blackberry". http://www.kaskus.us/showthread.php?t=6931696*. Akses Terakhir: 17 Maret 2011 pukul 08:46.

[3]. Munir, Rinaldi. 2007. *Kriptografi.* Bandung: Penerbit Informatika.

[4]. Wikipedia. *Kriptografi.* http://id.wikipedia.org/wiki/Kriptografi. Akses Terakhir: 17 Maret 2011 pukul 07:17.

[5]. Putro, Hanson Prihantoro. Percobaan Pemanfaatan Graf pada Protokol Kriptografi. Program Studi Teknik Informatika STEI ITB, Bandung 40135

[6]. Wikipedia. *BlackBerry.*http://id.wikipedia.org/wiki/BlackBerry. Akses Terakhir: 16 Maret 2011 pukul 09:28.

[7]. Juju, Dominikus dan Mata Maya Studio. 2009. *Bukan BlackBerry Biasa*. Jakarta: PT Elex Media Komputindo.

[8]. http://www.quora.com/What-is-the-protocol-for-Blackberry-Messenger. Akses terakhir: 19 Maret 2011 pukul 6.31.