REVIEW: METODE PENGAMANAN DATA PADA *PUBLIC INSTANT MESSENGER*

Putra Wanda
Program Studi Sistem Informasi
Fakultas Sains dan Teknologi
Universitas Respati Yogyakarta
Jl. Laksda Adisucipto, KM.6.5, Depok, Sleman, Yogyakarta, Indonesia
Email : wpwawan@gmail.com

Abstrak –

Saat ini, perkembangan *Instant Messenger* sangat pesat, salah satu aspek yang menjadi perhatian adalah tentang keamanan pesan yang dikirim melalui *Mobile Instant Messenger* yang harus melewati jalur komunikasi internet. Ada banyak metode yang telah dikembangkan untuk meningkatkan aspek pengamanan data meliputi penggunaan algoritma kriptografi keamanan seperti RSA-Triple DES, penggunaan algoritma AES pada protokol *Off The Record (OTR),* penggunaan algoritma Kurva *Hyper Elliptic* serta penggunaan jaringan virtual pada skema pengamanan.

Pada umumnya arsitektur komunikasi *Instant Messenger* dapat dibagi menjadi dua arsitektur yaitu arsitektur *client server* dan *peer to peer (P2P).* Makalah ini mendeskripsikan berbagai metode pengamanan yang telah dikembangkan untuk meningkatkan keamanan komunikasi pada *Public Instant Messenger*.

Kata Kunci : Algortima, Keamanan, *Mobile Banking*

PENDAHULUAN

Instant Messenger (IM) merupakan sebuah aplikasi yang banyak digunakan untuk melakukan pertukaran pesan melalui jaringan internet. Penggunaan public IM menjadi sangat pesat karena faktor *social presence, flow* dan *self-disclosure* (S. Park, 2014)

Jenis pesan yang paling sering dikirim melalui Mobile IM adalah pesan teks dan multimedia. Oleh karena itu aspek keamanan pesan menjadi hal yang sangat penting untuk diperhatikan (Lee, Y.H, 2014). Saat ini, Android menjadi salah satu sistem operasi yang banyak digunakan untuk komunikasi *public* IM, salah satu aplikasi terkenal adalah WhatApps untuk chatting komunikasi pribadi (Aglano, 2014).

Selain itu , penerapan public IM juga bisa dilakukan pada lingkungan perusahaan. Dalam hal ini, public IM digunakan untuk melakukan online interview terhadap karyawan yang akan bergabung pada perusahaan tersebut (Pearce, 2014).

Dengan banyak lingkungan penerapan *public* IM, maka aspek keamanan menjadi sangat penting. Enkripsi merupakan salah satu metode pengamanan pesan yang banyak digunakan pada aplikasi yang berjalan melalui jalur internet publik ini dimana enkripsi metode pengacakan pesan *plaintext* (asli) hingga menjadi sebuah *chippertext* (pesan acak) kemudian data yang tersebut akan dilewatkan melalui jaringan komunikasi global yaitu internet (Menezes, 1996).

Metode ini termasuk dalam disiplin kriptografi yang semakin berkembang saat ini. Meskipun demikian keamanan pesan melalui metode pengacakan data tidak menjamin keaslian pesan yang diterima karena metode autentikasi yang handal juga diperlukan pada proses mengetahui keaslian pesan (Schneier, 1996).. Sebuah layanan bisa dikatakan aman jika memenuhi beberapa unsur keamanan yang meliputi: kerahasiaan data, integritas data, otentikasi, Anti Penyangkalan (*Non Repudiation*) dan akses kontrol (A. Behrouz. 2008.)

Komunikasi menggunakan pesan IM sudah berkembang sejak lama dimana sistem komunikasi IM berbasis *client server* telah berkembang lebih dahulu. Sistem ini dijalankan dengan memperhatikan aspek komunikasi yang handal dan aman, hal ini dilakukan dengan mengharuskan seorang client untuk melakukan registrasi dan melalui proses autentikasi sistem sebelum dapat bergambung dalam jaringan IM. Sedangkan jalur komunikasi IM untuk komunikasi langsung juga bisa dilakukan melalui GPRS (U. Ali, 2005)

Pertumbuhan IM yang semakin pesat menyisakan resiko keamanan yang signifikan dan IM publik yang digunakaan saat ini kebanyakan tidak memiliki ketentuan untuk menjamin kerahasiaan pesan yang dikirim menggunakan aplikasi IM. Oleh karena itu, sebuah model *public* IM berbasis SIMPC (*Secure Instant Messaging and Presence Control*) yang dikombinasikan dengan metode *elliptic-curve cryptography* telah dikembangkan (Chung, 2008)

Penerapan keamanan pada *public* IM pada lingkungan Publik harus didukung dengan keamanan yang baik dimana penggunaan firewall, inspeksi setiap paket, pembaharuan keamanan pada sistem dan isi menjadi hal yang sangat penting (Sullivan, 2006)

Pada penerapan IM hal yang sering menjadi pilihan adalah dimana lingkungan IM akan dijalankan. Lingkungan ini dapat bersifat publik atau menggunakan IM yang bersifat privat, hal ini tentu berhubungan dengan aspek keamanan aplikasi yang digunakan, Penggunakan IM publik dalam hal ini akan menggunakan sebuah *proxy* untuk melakukan penyaringan (*filtering*) pada lalu lintas data yang masuk dan keluar melalui IM (Casey, 2007)

1. Risiko keamanan Public IM

Ada beberapa kasus yang menunjukkan risiko keamanan pada IM baik yang terjadi pada IM privat atau IM yang digunakan oleh publik. Sistem yang lemah akan memudahkan penyerang untuk menyebarkan pesan palsu atau *worm* yang dapat merusak perangkat mesin pada perusahaan yang menggunakan IM.

Selain itu juga terdapat banyak jenis serangan yang telah dilakukan oleh penyerang sehingga menimbulkan bahaya pada sistem sehingga hal ini tentu menjadi perhatian para pengembang. Bahaya-bahaya yang ditimbulkan bisa ditampilkan pada Tabel 1:

Tabel 1 : Risiko Penggunaan Aplikasi IM

NO	Bagian yang berisiko	Bentuk Ancaman
1	Kehilangan kontrol terhadap *Malicious Code*	Trojan dan Virus
2	Komunikasi yang tidak dienkripsi	Penyadapan
3	Kurangnya kontrol pada trafik yang menuju keluar jaringan	Kehilangan informasi
4	Autentikasi yang lemah	Impersonasi
5	Kurangnya pengelolaan *password*	Pencurian identitas
6	Kebocoran informasi pribadi	Pelacakan
7	Kealfaan dalam mengontrol *log message*	Pencurian pesan log
8	Kealfaan dalam mengontrol hak cipta	Pelanggaran hak cipta
9	Kurangnya fungsi *backup* pesan	Penolakan pesan

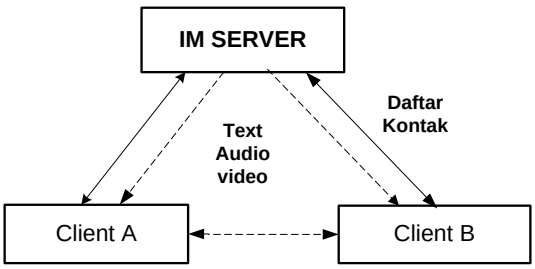
Berdasarkan data jenis resiko dan ancaman yang bisa terjadi pada sistem IM maka diperlukan solusi untuk menyelesaikannya. Sebagai sebuah sistem teknologi yang bekerja secara *real time*, murah dan banyak digunakan, maka masalah keamanan sistem ini menjadi sangat penting Jika tidak dikelola dengan baik, IM dapat menjadikan informasi yang bersifat pribadi menjadi sangat berisiko tetapi jika pengelolaan dilakukan melalui kontrol keamanan yang baik dan terintegrasi dengan alur bisnis maka perusahaan dapat meningkatkan kemampuan untuk menjalankan perusahaan secara *real time* dengan dukungan IM(S. Kim, 2005)

Walaupun telah dilakukan kontrol keamanan yang baik dan terintegrasi dapat meningkatkan keamanan sistem IM, tidak dijelaskan tentang detail dari risiko

yang terjadi pada IM komersial dan lebih menonjolkan permasalahan teknis dibandingkan dengan permasalahan managerial

2. Keragaman Arsitektur pada Mobile IM

Arsitektur sistem IM yang banyak digunakan saat ini adalah komunikasi IM yang berbasis arsitektur *client-server* dan P2P. Pada komunikasi *client-server* semua pesan yang berasal dari pengirim harus melewati *server* sebelum sampai ke sisi penerima. Jika sistem ini hanya mengandalkan pada proses komunikasi IM berbasis *client-server*, hal ini akan melupakan aspek privasi dan kemungkinan pesan akan dibuka pada *server* setelah pesan tersebut dikirim dari pengirim hingga akhirnya sampai ke sisi penerima ataupun sebaliknya. Oleh karena itu penerapan IM menggunakan sebuah model protokol yang dianggap aman bernama SIMPP (*Secure Instant Messaging and Privacy Presence)* untuk membangun sebuah model komunikasi 3-way pada metode *elliptic-curve cryptography*. Model komunkasi 3-way ini bekerja sebagaimana diilustrasikan pada Gambar 1.

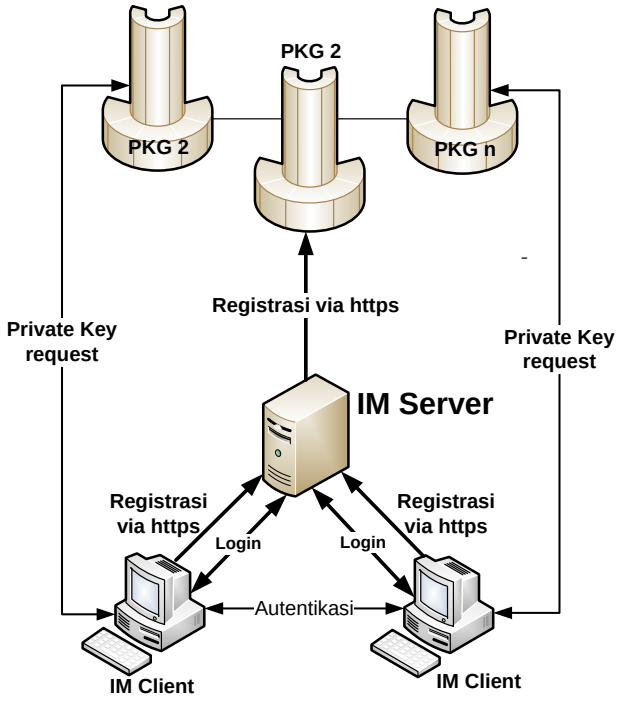


Gambar 1 : Arsitektur Komunikasi Client Server

Pada model komunikasi 3-way ini, komunikasi data antara dua *client* harus melewati *server* sehingga pertukaran pesan dianggap lebih aman. Pada sistem IM 3-way ini, model komunikasinya dianggap aman karena hanya client yang berada pada kontak list yang bisa berkomunikasi Namun demikian proses monitoring keamanan user yang aktif pada sistem 3-Way ini menjadi tidak konsisten karena tidak memiliki proses autentikasi yang jelas pada saat *client* yang lain ingin memasuki sistem IM.

Sistem komunikasi 3-way yang masih memiliki celah pada keamanan pesan membuat arsitektur *client-server* yang dirancang untuk komunikasi IM dilakukan dengan menambahkan *Private Key Generator* (PKG) yaitu sistem komunikasi IM yang terdiri dari komponen IM *Client*, IM *Server* dan PKG..

Pada sistem ini IM *server* bertugas untuk melakukan pemeriksaan terhadap semua pengguna pada sistem dan memberikan akses kepada pengguna yang valid untuk menggunakan sumber daya yang ada dan IM *Client* akan digunakan untuk mengirim pesan sesuai dengan daftar kontak yang dimiliki. Sedangkan PKG berfungsi untuk melakukan pengaturan parameter sistem, membangkitkan sebuah identitas berdasarkan private key untuk IM Client (Wang, 2013). Sistem berbasis PKG ini dapat diilustrasikan pada Gambar 2.



Gambar 2 : Arsitektur sistem IM berbasis PKG

Meskipun arsitektur sistem IM berbasis PKG ini dapat meningkatkan keamanan IM *server* dan IM *Client*, tetapi risiko akan timbul jika proses pada PKG ini mengalami kegagalan. Hal ini tentu akan mengakibatkan kebocoran data pada sistem IM.

Penerapan sistem IM dengan menggunakan arsitektur *client-server* juga telah dilakukan dengan memanfaatkan protokol Jabber. Protokol Jabber dapat bekerja pada sistem IM dan berbasis arsitektur koneksi *client-server*. Arsitektur yang memanfaatkan protokol ini memiliki bentuk operasi yang mirip dengan operasi *email* dimana masing-masing penguna memiliki *server* bersifat lokal yang digunakan untuk menerima pesan-pesan. Berbagai macam server ini akan berkomunikasi dengan server yang lain jika ingin mengirimkan sebuah informasi ke pengguna. Setiap komunikasi yang berasal dan menuju ke *client* akan melewati sebuah *server*, data-data pengguna yang meliputi daftar kontak dan *preference* akan disimpan di dalam server lokal . Arsitektur ini dianggap lebih aman untuk membangun sebuah sistem IM (Serik, 2014)

Pada umumnya aspek keamanan pada komunikasi *client* dan *server* dianggap riskan baik pada saat *client* ingin mengirim data ke *server* lokal ataupun ketika pengguna ingin mengirim pesan IM yang harus melewati banyak server lokal. Sistem *client-server* berbasis *server* lokal ini akan meningkatkan peluang terjadinya penyadapan.

Dengan perkembangan teknologi komunikasi yang sangat pesat, pendekatan lain yang memungkinkan untuk membangun sebuah sistem IM adalah dengan menerapkan arsitektur komunikasi P2P dengan memanfaatkan teknologi JXTA dan JXME. Teknik komunikasi yang dilakukan dengan arsitektur P2P ini dijalankan dengan konsep "*Message Passing*" dimana aplikasi memberikan layanan *presence* yang dapat menunjukkan dalam periode waktu tertentu. Sebuah *peer* akan mengirimkan "*Alive Message*" yaitu berupa pesan kondisi *peer* setiap beberapa waktu. Ketika sebuah *peer* tidak dapat menerima *Alive Message* dalam waktu 10 detik maka *peer* tersebut dianggap sudah padam dan semua informasi percakapan akan dihapus (Tahsin, 2008)

Penerapan arsitektur komunukasi berbasis P2P juga telah diteliti sebelumnya, terutama dalam hal penggunaan metode enkripsi pada komunikasi IM dimana solusi yang ditawarkan adalah metode *Broadcast Encryption* (BE). Metode BE dianggap memiliki performa yang tinggi dalam hal proses enkripsi dan dekripsi tanpa harus dibatasi oleh jumlah identitas atau grup. Sehingga dapat menciptakan enkripsi yang lebih efisien (Bodriagov, 2009)

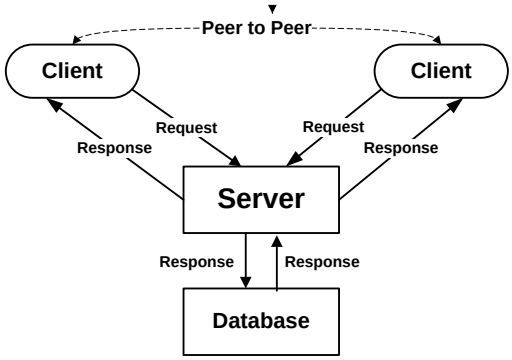
3. Model pengamanan pada Instant Messenger

Perkembangan IM yang sangat pesat menghasilkan berbagai model pengamanan sistem yang dianggap lebih baik. Salah satu dari model yang dikembangkan untuk meningkatkan keamanan sistem adalah dengan menerapkan sebuah model berupa sistem IM yang berdasarkan pada *Spim detection* dan *filtering*. Model ini dilakukan dengan menerapkan daftar *Black/White* dimana paket data yang dikirim akan terlebih dahulu diperiksa sumber dan tujuannya untuk memerika validitas serta melakukan penyaringan terhadap pesan *spam* yang melewati sistem IM. Pada sistem ini *client* akan membuat sebuah *pipeline* dengan memproses pesan masuk setelah melakukan *checking error* dan *filtering*. Pemeriksaan kesalahan dan penyaringan dilakukan untuk menentukan apakah data tersebut akan dikategorikan sebagai daftar *Black/White* atau tidak (Zhijun, 2005)

Sebagai aplikasi Internet yang sangat berkembang saat ini beberapa kelemahan pada keamanan menjadi penghalang tersendiri bagi IM sehingga diperlukan metode pengamanan pada level

sistem. Model pengamanan ini dilakukan dengan mengkripsi semua proses sebelum data ditransmisikan. Ketika *client* menerima data *chippertext* maka data akan didekripsikan menggunakan kombinasi algoritma RSA dan Triple DES (Wenping, 2009)

Model pengamanan IM ini dapat diilustrasikan pada gambar 3.



Gambar 3 : Model pengamanan berbasis RSA dan Triple DES

Model pengamanan berbasis RSA dan Triple DES ini menjadi lebih aman karena pesan telah mengalami proses enkripsi sebelum ditransmisikan melalui Internet. Meskipun demikian permasalahan akan muncul ketika terjadi pertukaran data yang semakin besar, hal ini menyebabkan kecepatan komputasi menjadi semakin lambat apalagi jika mentrasmisikan data yang berupa suara, video atau gambar

Beberapa metode pengamanan lain telah diusulkan dalam bidang komunikasi data melalui *Mobile* IM berbasis arsitektur P2P. Sebagian besar metode pengamanan yang diusulkan berfokus pada penggunaan algoritma fungsi Hash pada pesan *Mobile* IM. Fungsi Hash yang diterapkan pada pesan digunakan untuk melakukan pengamanan pesan *plaintext* yang dikirim melalui jaringan Internet.

Pengembangan metode pengamanan pesan yang dilakukan ,melalui penerapan fungsi Hash pada data yang akan ditransmisikan melalui IM dimana pesan teks dianggap lebih cocok untuk menggunakan enkripsi tipe *Secure Hash Algoritm*(SHA). Penerapan metode ini dilakukan dengan menentukan sebuah fungsi F(M) dimana nilai M adalah panjang pesan IM yang bisa berubah-ubah. Ada dua tipe pengkodean pesan yang penting pada sistem ini yaitu: *checksum* dan *secure hash*. *Checksum* merupakan sebuah fungsi dari message M yang pada dasarnya hanya memiliki satu *property* sehingga nilai F(M) tergantung pada semua *byte* yang ada pada M. Dengan memanfaatkan metode ini pesan yang dikirim melalui jalur internet dianggap lebih aman (Yusof, 2011).

Namun satu hal yang menjadi catatan adalah tipe pesan M yang pada sistem ini hanya terdiri dari M1 dam M2 tentu sangat riskan sebab kode yang dibangkitkan untuk pertama kalinya bisa terdeteksi dengan lebih mudah.

Metode pengamanan IM dapat juga dilakukan pada level protokol. Salah satu protokol yang banyak diterapkan pada sistem IM adalah Jabber. Protokol ini memiliki keunggulan antara lain: Terbuka, terstandadisasi, aman dan protokol ini didesain yang bisa dikembangkan. Berdasarkan sifatnya yang terbuka, Jabber banyak digunakan untuk membangun model pengamanan pada IM.

Selain itu untuk meningkatkan keamanan pesan IM, maka dikembangkan sebuah protokol yang terbentuk dari kombinasi ElGamal *cryptosystem*, algoritma RSA, and *Chinese Remainder Theorem* (CRT). Pada protokol ini bagian CRT lebih berperan pada pembaharuan *private key* pengguna sedangkan kemampuan berinteraksi antar algoritma ini tergantung pada *integer factorization problem* (IFP) dan *discrete logarithm problem* (DLP).

Metode yang diusulkan diatas dianggap memiliki tingkat keamanan yang lebih baik dan cepat (Mohamed, 2011). Meskipun demikian, model pengamanan di atas tidak memberikan autentikasi pada pesan yang diterima.

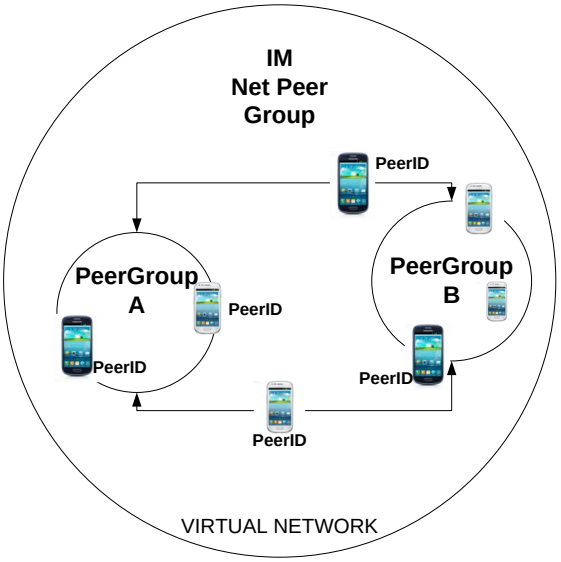
Seiring dengan perkembangan aplikasi pengiriman pesan IM, telah dikembangkan metode pengamanan menggunakan sistem kriptografi berdasarkan identitas dapat memberikan autentikasi yang cukup baik dan komunikasi yang lebih aman pada sisi *server* dan *client*. Sistem yang dibangun menggunakan onsep kriptografi berdasarkan identitas ini dianggap bisa menghasilkan sistem IM yang lebih sederhana dan efisien dibandingkan dengan sistem yang sudah ada.

4. Kriptografi pada Pesan Instant Messaging

Penemuan kelemahan pesan melalui analisa data dan *sniffing* menuntut pengembangan metode keamanan yang lebih baik pada sistem IM sehingga dapat menjaga integritas data dan tidak mengalami perubahan pada saat data diterima oleh penerima.

Dalam perkembangan dunia internet abad ke-21 berbagai macam teknik telah dikembangkan untuk mengamankan pesan IM. Pada saat ini bentuk enkripsi yang digunakan bekerja dengan memanfaatkan algoritma enkripsi simetris dan asimetris untuk mengamankan sebuah pesan. Meskipun demikian, beberapa IM publik bersifat komersial saat ini ternyata tidak melakukan proses enkripsi pesan sama sekali ketika melakukan pengiriman pesan melewati jalur internet dengan kata lain, pesan dibiarkan terbuka (*plaintext*) . Hal ini tentu sangat riskan terhadap aksi kejahatan (Barghuthi, 2013)

Selain itu, perkembangan IM yang pesat menuntut penggunaan protokol yang aman dalam melakukan komunikasi data. Pendekatan melalui protokol *Off The Record* (OTR) telah dilakukan untuk meningkatkan keamanan pesan tersebut, protokol ini bekerja dengan memanfaatkan enkripsi yang cukup kuat yaitu dengan algoritma kunci simetri AES, pertukaran kunci menggunakan konsep Diffie Helman, menggunakan fungsi Hash SHA-1, Dengan konsep komunikasi berbasis OTR, aplikasi IM menyediakan dukungan dalam pengiriman pesan IM yang bersifat privat. Metode ini pengamanan dimulai sejak user mengaktifkan OTR. Setelah OTR diaktifkan, pengguna IM dapat menggunakan saluran komunikasi khusus yang terenkripsi (Nalawade, 2014). Selan itu juga, metode pengamanan instant messenger juga bisa dilakukan menggunakan skema jaringan virtual berbasis arsitektur peer- to peer (Wanda, 2014). Penggunaan jaringan virtual akan memberikan keamanan pada pengiriman pesan yang melewati jaringan publik. Skema pengamanan berbasis virtual network di atas bisa dilihat pada gambar 4.



Gambar 3 : Skema pengamanan dengan Jaringan Virtual

Sebuah metode pengamanan lain untuk public IM berbasis kriptografi kunci publik juga telah dilakukan. Penelitian ini (Wanda, 2014) telah mengajukan sebuah metode pengamana berbasis kriptografi Kurva *Hyper Elliptic*. Pengamanan dilakukan dengan menggunakan skema pengamanan tanda tangan digital dan skema enkripsi-dekripsi. Keunggulan dari metode ini adalah akan memberikan aspek keamanan sekaligus yaitu aspek keaslian, integritas dan kerahasiaan pada pesan *Public* IM yang melewati internet.

5. Ringkasan

Perkembangan IM yang pesat memunculkan berbagai risiko yang bisa terjadi kapan saja. Risiko akibat lemahnya sistem IM yang digunakan antara lain: Kehilangan informasi, Impersonasi, pencurian identitas, pencurian *Message Log* dan pelanggaran hak cipta.

Makalah ini mendeskripsikan berbagai model, metode dan arsitektur yang digunakan untuk pengamanan *public* IM. Di dalam membangun sistem IM, asitektur yang banyak digunakan adalah arsitektur berbasis *client-server* dan *peer-to-peer*. Arsitektur *client-server* bekerja dengan memanfaatkan *server* sebagai pusat komunikasi dan manajemen IM, sedangkan sistem berbasis arsitektur P2P lebih mengedepankan komunikasi langsung antar *peer* tanpa harus tergantung pada \ *server*. Penerapan IM berbasis *client-server* dan P2P juga memiliki kelebihan dan kelemahan masing-masing.

Di dalam membangun sistem IM yang aman, beberapa model pengamanan meliputi: penggunaan kombinasi RSA dan Triple DES, pengamanan menggunakan fungsi Hash hingga menggunakan protokol IM yang dianggap aman yakni protokol Jabber. Meskipun demikian, pengamanan dengan menggunakan kombinasi tanda tangan digital dan kriptografi yang efisien masih memerlukan penelitian lanjut.

REFERENSI

[1] Menezes A., Van Oorschot P, & Vanstone S. "Handbook of Applied Cryptography". *CRC Press Inc*. 1996.

[2] Scheiner B. "Applied Cryptography Protocols, Algorithms and Source Code in C. Second Edition." New York: *John Wiley & Sons,inc*, 1996.

[3] Forouzan, A Behrouz. "Cryptography and Network Security. Singapore," *Mc Graw-Hill Education (Asia)*, 2008

[4] U. Ali, S. J. Nawaz, A. G. K. Jadoon, and S. A. Khan, “Mobile-to-mobile IM: A real time chatting system for GPRS networks,” 2005, vol. 2005, pp. 92–97

[5] Kim and C. S. Leem, “Security of the internet-based instant messenger: Risks and safeguards,” *Internet Res.*, vol. 15, no. 1, pp. 88–98, 2005.

[6] Zhijun. L, Weili, Nal L and David.L, “Detecting and Filtering Instant Messaging Spam – A Global and Personalized Approach,” IEEE 2005

[7] O’Sullivan, “Instant Messaging vs. instant compromise,” *Netw. Secur.*, vol. 2006, no. 7, pp. 4–6, 2006.

[8] D. Casey, “Building a secure instant messaging environment,” *Netw. Secur.*, vol. 2007, no. 1, pp. 18–20, 2007.

[9] Chung. H. Y, Tzong. Y. K, TaeNam. A and Chia-Pei. L, “Design and Implementation of a Secure Instant Messaging Service based on Elliptic-Curve Cryptography,” *Journal of Computers* Vol.18, No.4, January 2008.

[10] T. Tahsin, L. F. Choudhury, and M. L. Rahman, “Peer-to-peer mobile applications using JXTA/JXME,” 2008, pp. 702–707.

[11] Wenping Guo, Zhenlong L, Ying C, Xiaoming Z,“Security Design for Instant Messaging System Based on RSA and Triple DES,” *2009 IEEE*

[12] Yusof. M. K and Faisal A. A, “A Secure Private Instant Messenger,” .2011

[13] Bodriagov. O and Sonja. B, “Encryption for Peer-to-Peer Social Networks.”, pp. 258–262, 2011.

[14] Mohamed H. E, Khaled A, Muhammad K. K, Hassan E. “Secure Instant Messaging Protocol for Centralized Communication Group,”. 2011.

[15] C.-J. Wang, W.-L. Lin, and H.-T. Lin, “Design of an instant messaging system using identity based cryptosystems,” 2013, pp. 277–281.

[16] M. Serik and G. B. Balgozhina, “Instant messaging application for smartphone,” *Life Sci. J.*, vol. 11, no. SPEC.ISS.1, pp. 258–262, 2014.

[17] N. B. Al Barghuthi and H. Said, “Social networks IM forensics: Encryption analysis,” *J. Commun.*, vol. 8, no. 11, pp. 708–715, 2013.

[18] A. Nalawade, D. Kamdar, P. Angolkar and S. Gaikwad, “Integrated Instant Messaging System,” IJLTET. *J.*, vol. 3, ISSN: 2278-621X, 2014.

[19] Park, K. Cho, and B. G. Lee, “What makes smartphone users satisfied with the mobile instant messenger?: Social presence, flow, and self-disclosure,” *Int. J. Multimed. Ubiquitous Eng.*, vol. 9, no. 11, pp. 315–324, 2014.

[20] Lee, Y.H., Park, K.J., Jin, C.Y., Kim, D.G. The explanation of mobile instant messenger dependence focusing on media and message attributes (2014) Information (Japan), 17 (7), pp. 33513356.

[21] Anglano, C. Forensic analysis of whats app messenger on Android smartphones (2014) Digital Investigation, 11 (3), pp. 201213.

[22] P. Wanda, Selo and B. S. Hantono, "Model of secure P2P mobile instant messaging based on virtual network," *Information Technology Systems and Innovation (ICITSI), 2014 International Conference on*, Bandung, 2014, pp. 81-85.

[23] Pearce, G., ThøgersenNtoumani, C., Duda, J.L. The development of synchronous textbased instant messaging as an online interviewing tool (2014) International Journal of Social Research Methodology, 17 (6), pp. 677692.

[24] P. Wanda, Selo and B. S. Hantono, "Efficient message security based Hyper Elliptic Curve Cryptosystem (HECC) for Mobile Instant Messenger," *Information Technology, Computer and Electrical Engineering (ICITACEE), 2014 1st International Conference on*, Semarang, 2014, pp. 245-249.