EFISIENSI PENGAMANAN PESAN *MOBILE BANKING* BERBASIS ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES)

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, penerapan Mobile Banking untuk transaksi keuangan semakin meningkat, hal ini disebabkan oleh meningkatnya jumlah pengguna perangkat bergerak dalam melakukan transaksi perbankan. Penelitian ini dilakukan untuk meningkatkan keamanan pesan Mobile Banking dengan memanfaatkan algoritma Advanced Encryption Standard (AES) dengan menggunakan beberapa parameter keamanan pada skema AES. Hal ini dilakukan untuk mewujudkan transaksi yang aman dan efisien dengan penerapan metode kriptografi pada pesan. Hasil yang dicapai dalam penelitian ini adalah terciptanya suatu aplikasi berbasis Android yang dapat digunakan untuk melakukan transaksi Mobile Banking dengan penambahan algoritma AES. Penelitian ini menghasilkan waktu komputasi yang cukup cepat dan efektif pada aplikasi M-Banking berbasis Android.

Kata Kunci : Algoritma AES, Keamanan, Mobile Banking

1. Pendahuluan

Teknologi bergerak saat ini sudah menjadi tren perkembangan teknologi informasi masa kini. Teknologi ini juga diperkirakan akan mengalami perkembangan yang pesat di masa mendatang Dengan semakin banyaknya perangkat *mobile* yang bisa berfungsi seperti sebuah komputer, ini mengindikasikan bahwa perkembangan teknologi ke arah *Mobile Technology* semakin nyata.

Android merupakan salah satu Sistem Operasi yang banyak digunakan untuk perangkat bergerak yang telah menjadi salah satu tren teknologi modern. Dengan fitur-fitur baru yang mendukung untuk perangkat *Mobile* serta keunggulan yang dimilikinya, Android dapat menjadi salah satu solusi yang cocok untuk pembangunan sebuah aplikasi pada perangkat bergerak seperti sebuah ponsel atau sebuah perangkat Smartphone. Tetapi, aspek keamanan pada sistem operasi Android masih banyak ditemukan, terutama dengan munculnya berbagai serangan berupa virus dan *malware* terhadap sistem operasi Android (F. Paruki, 2015)

Seiring dengan pesatnya penggunaan mobile internet, banyak transaksi perbankan beralih dari *Internet Banking* berbasis Web menjadi *Mobile Banking* berbasis *Fully Mobile*.
Sehingga dengan pesatnya perkembangan tersebut, maka kebutuhan aka aspek keamanan makin tinggi terutama untuk transaksi yang dilakukan melalui perangkat berbgerak. Pada *Mobile Banking,* aspek keamanan data pada sisi pengguna maupun proses pengiriman pesan menjadi salah satu aspek yang sangat penting. Perangkat *mobile* saat ini banyak digunakan untuk mendukung berbagai aktifitas manusia seperti *chatting*, *browsing* hingga melakukan pembayaran transaksi (BAC Review, 2014)

Kriptografi (*Cryptography*) merupakan istilah kata yang berasal dari dua buah kata dalam bahasa Yunani yaitu *crypto* dan *graphia* yang berarti penulisan rahasia atau ilmu yang mempelajari tentang penulisan secara rahasia. (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.)

Aspek keamaman data dengan skema kriptografi yang menjadi unsur pembentuk sebuah sistem keamanan terdiri dari beberapa aspek yaitu:

1. *Privacy/ Confidentiality*
2. *Integrity*
3. *Authentication*
4. *Non-repudiation*

Saat ini hampir 62% Bank di seluruh dunia telah menerapkan Mobile Banking dalam layaaannya kepada pelanggan. Tetapi, sejumlah 72% Bank yang menerapkan layanan Mobile Banking masih khawatir dengan aspek keamanan dari layanan yang diberikan tersebut. Hal ini tentu memerlukan solusi dari aspek penerapan teknologi yang akan digunakan pada layanan Mobile Banking tersebut (Vasco, 2009)

Bahaya keamanan layanan M- Banking ini banyak berasal dari aspek non teknis. Misalnya, sebuah bahaya dari penggunaan M-Banking bisa terjadi ketika ada pihak ketiga mengetahui nomor PIN dari

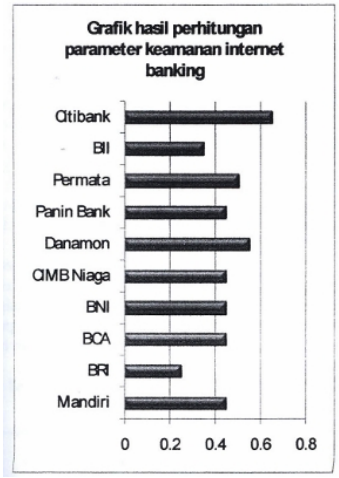
seorang pengguna *mobile banking*. Adapun peluang itu dapat muncul dari operator atau pada orang terdekat sendiri. Ketika operator yang digunakan mengetahui nomor PIN pengguna ataupun *password* yang digunakan maka aspek keamanan data menjadi hal yang riskan (Kus Ikhsanto, 2010)

Meskipun demikian, motivasi pengguna dalam menggunakan layanan *mobile banking* bisa dikatakan baik. Apalagi dengan dukungan berbagai fitur dalam mobile banking yang memberikan kemanfaatan, kemudahan dalam penggunaan, dan kualitas layanan yang baik membuat layanan transaksi berbasis *mobile* ini semakin diminati oleh berbagai kalangan pengguna (Shih, 2015)

Pada penelitian, aspek pengamanan data akan menggunakan skema kriptografi dengan memanfaatkan algoritma *Advanced Encryption Standard* (AES). AES merupakan standar baku kriptografi yang telah disahkan oleh lembaga *National Institute of Standards and Technology* (NIST) yang banyak digunakan untuk membangun standar pengamanan aplikasi/layanan (FIPS, 2001).

Penelitian Terkait

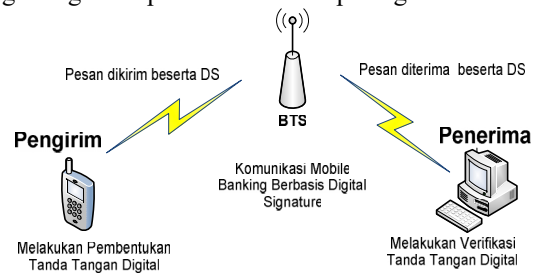
Di Indonesia, sebuah penelitian tentang Internet Banking telah dilakukan untuk melakukan analisa tentang metode pengamanan yang digunakan oleh beberapa Bank Nasional dalam mengelola transaksi Internet Bankingnya. Hasil penelitian tentang tingkat pengamanan internet banking bisa dilihat pada gambar 1.



Gambar 1 Tingkat pengamanan *Internet Banking* pada Bank

Berdasarkan hasil pengamatan dari tabel parameter 10 bank yang ada di indonesia. Bank mandiri, BCA, BNI, CIMB Niaga, Panin Bank, dan Permata memiliki tingkat keamanan yang hampir sama kedudukannya. Akan tetapi BRI memiliki tingkat keamanan yang kurang karena internet banking BRI tidak memiliki *suport hardware* semacam Token PIN. Internet Banking kedua yang kurang aman adalah BII karena bank ini hanya memiliki SMS Token (Ikhsanto, Amalia, 2010).

Penelitian lain yang telah dilakukan dalam membangun sistem keamanan *Mobile Banking* adalah dengan menerapkan tanda tangan digital berbasis SHA (*Secure Hash Algorithm*) pada aplikasi SMS Banking. Skema komunikasi *Mobile Banking* dengan menggunakan teknik pengamanan tanda tangan digital dapat diilustrasikan pada gambar 2.



Gambar 2 Ilustrasi Komunikasi SMS Banking dengan SHA

Dari analisa yang didapatkan, penelitian ini menyimpulkan bahwa pemberian tanda tangan digital terhadap sebuah pesan dapat dilakukan terhadap pesan SMS melalui perangkat seluler. Untuk itu hal ini sangat memungkinkan untuk dapat diterapkan dalam proses transaksi SMS Banking dimana sistem keamanan SMS Banking saat ini masih mempunyai kekurangan dalam keamanan di level non teknis.(Budiono, 2009).

Penelitian lain juga telah diajukan untuk meningkatkan keamanan transaksi internet banking. Penelitian ini mengajukan metode pengamanan internet banking berbasis multi biometrik. Metode multi biometrik yang diajukan berupa kombinasi pengamanan internet banking melalui penerapan *token* dan *fingerprint*. Proses kerja sistem ini adalah dengan melakukan pemeriksaan *token* dan *fingerprint* setiap kali pengguna ingin melakukan transaksi perbankan (Catalin et al, 2015). Sistem diatas bisa diilustrasikan pada Gambar 3.

Gambar 3 Ilustrasi pengamanan internet Banking dengan multi biometrik

Selain itu, metode lain yang diajukan untuk meningkatkan keamanan *mobile banking* adalah dengan menerapkan *One Time Password* (OTP) yang digunakan dalam proses enkripsi dan dekripsi pesan pada proses transaksi pesan antara client dan server. Penerapan metode OTP ini digunakan untuk mencapai pengamanan berbasis *end-to-end authentication* (B. Singh, 2015)

Algoritma AES

Advanced Encryption Standard merupakan salah satu algoritma dalam kriptografi modern [Daemen, 1998]. Algoritma AES merupakan dalam satu

algoritma simetris yang banyak digunakan dalam bidang pengamanan data (Viega, 2002).

Selain itu juga, AES banyak digunakan dalam pengamanan sistem komunikasi saat ini, *Advanced Encryption Standard* (AES) merupakan standar enkripsidengan kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat (IEEE Stand Ass, 2012).

Standar ini terdiri atas 3 blok cipher, yaitu AES-128, AES-192 and AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Masing-masing cipher memiliki ukuran 128-bit, dengan ukuran kunci masing-masing 128, 192, dan 256 bit. AES telah dianalisis secara luas dan sekarang digunakan di seluruh dunia, seperti halnya dengan pendahulunya, *Data Encryption Standard (DES)* (Stalling, 2006)

Algoritma AES bekerja dengan konsep *round* berbasis tabel, sehingga pemilihan blok *table round* akan mempengaruhi memory dan overhead yang terjadi pada saat melakukan komputasi pada perangkat *wireless* seperti pada *mobile phone* (X.-Q. Luo, 2015)

Input dan *output* dari algoritma AES terdiri dari urutan data sebesar 128 *bit*. Urutan data yang sudah terbentuk dalam satu kelompok 128 *bit* yang disebut sebagai blok data atau *plaintext* yang nantinya akan dienkripsi menjadi *ciphertext*. *Cipher key* dari AES terdiri dari *key* dengan panjang 128 *bit*, 192 *bit*, atau 256 *bit*. Perbedaan panjang kunci akan mempengaruhi jumlah *round* yang akan diimplementasikan pada algoritma AES ini. Tabel 1 dibawah ini akan memperlihatkan jumlah *round* putaran (Nr) yang harus diimplementasikan pada masingmasing panjang kunci.

Tabel 1 Jumlah *Round* dan *Key* pada algoritma AES

	Jumlah Key (Nk)	Ukuran Block (Nb)	Jumlah Putara (Nr)
AES – 128	4	4	10
AES – 192	6	4	12
AES – 256	8	4	14

Berdasarkan tabel 1 di atas, dapat dideskripsikan bahwa panjang kunci dalam algoritma AES memiliki jumlah jumlah putaran (*round*) yang berbeda beda. Semakin panjang kunci yang digunakan, maka jumlah putaran akan semakin banyak.

Pada penelitian ini, digunakan berbagai simulasi perangkat *mobile* yang berbeda-beda. Saat ini, perangkat digunakan dalam proses transaksi *mobile banking* saat ini sebagian besar memiliki *resource* yang terbatas, sehingga dilakukan berbagai pendekatan untuk mempercepat kemampuan dan waktu komputasi untuk penerapan algoritma AES, termasuk dengan menggunakan *hardware accelerators* (Rahimunnisa, Morioka,2013).

Selain itu, skema untuk mempercepat kinerja AES bisa dilakukan pada sistem tertanam (Q. Yue, 2015) ataupun menggunakan teknik Software optimizations (Bertoni, Gladman, Atasu, 2003)

Pengajuan Metode Pengamanan

Kriptografi adalah salah satu teknik yang sangat banyak digunakan untuk membangun sebuah informasi yang aman, kriptograf digunakan untuk mengubah sebuah teks asli *(plaintext)* menjadi teks berkode *(ciphertext)* dan sebaliknya. Pada konsep kriptografi, enkripsi digunakan untuk mengubah *plaintext* menjadi *ciphertext* dan dekripsi digunakan untuk mengubah *ciphertext* menjadi *plaintext*. Proses enkripsi dan dekripsi membutuhkan sebuah kunci/sepasang kunci (Menezes, 1996)

Model pengamanan

Pada penelitian ini metode pengamanan komunikasi mobile banking akan menerapkan algoritma AES dengan berbagai varian kunci yang meliputi panjang kunci 128, 192 dan 256 bit.

Pendekatan komunikasi yang digunakan pada penelitian ini adalah dengan dengan model arsitektur berbasis *client server*. Pada saat ingin melakukan transaksi penbankan melalui *mobile banking*, seorang client harus terlebih dahulu meminta kepada *server* sebuah kunci yang akan digunakan untuk melakukan komunikasi.

Pada sisi *client*, setiap pengguna yang hendak mengirim pesan melalui jaringan publik (internet) terlebih dahulu harus melakukan enkripsi pada pesan tersebut dengan menggunakan skema algoritma *Advanced Encryption Standard.*

Sedangkan pada sisi *server*, pesan yang sudah diberikan pengamanan menggunakan algoritma AES pada *user* akan melakukan komunikasi dengan client tersebut menggunakan *session key* yang sudah disepakati sebelumnya.

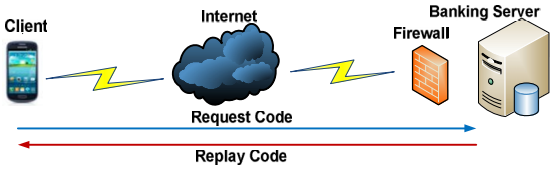
Tahap Pengamanan

Pada penelitian ini penerapan algoritma AES digunakan selama sesi komunikasi antara *client* dan *server* bank. Dalam proses pengamanan pesan *mobile banking*, ada beberapa tahap yang harus dilalui pada sisi *client* maupun *server*, tahap-tahap pengamanan yang dilalui antara lain:

- **Tahap memulai komunikasi**

  Pada tahap ini, *client* akan melakukan *request* kepada *server* untuk meminta kode pembangkitan kunci yang akan digunakan untuk melakukan komunikasi dalam sebuah sesi. Pada tahap ini, server akan mengirimkan sebuah kode acak kepada setiap *user* dan merekan identitas pengguna yang melakukan permintaan kode. Setelah kode diterima oleh *client*, kode akan digunakan untuk membangkitkan kunci yang akan digunakan untuk mengamankan komunikasi yang terjadi selama sesi berlangsung.

Tahap permintaan kode oleh *client* yang akan digunakan untuk pembangkitan kunci bisa diilustrasikan pada Gambar 4.



Gambar 4 : Transaksi Kode pada Mobile Banking

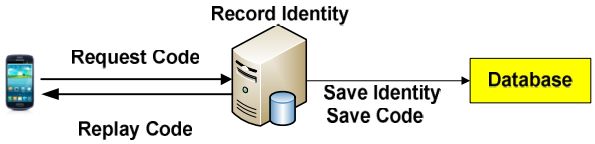
Dari gambar 4 dapat dideskripsikan bahwa setiap kali *client* ingin melakukan transaksi perbankan melalui jaringan publik, maka *client* harus melakukan aksi *request code* (permintaan kode tertentu kepada server).

- **Tahap pembangkitan kunci**
  Pada tahap ini, setiap client yang telah menerima random code dari server akan mulai membangkitkan kunci masing-masing dengan skema algoritma AES. Hasil dari pembangkitan kunci tersebut kemudian akan digunakan untuk melakukan komunikasi pesan. Proses pembangkitan kunci bisa diilustrasikan pada gambar 5.

Gambar 5 : Pembangkitan Kunci

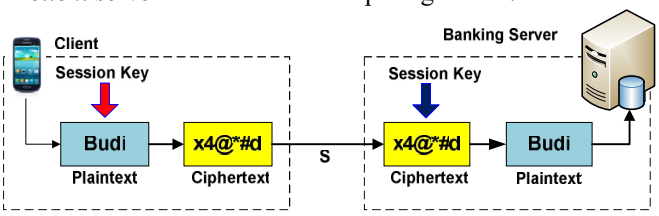
Kunci yang telah dibangkitkan tadi hanya bisa digunakan dalam sebuah sesi komunikasi, jika sesi transaksi data berakhir maka server akan menghapus kunci sehingga tidak bisa digunakan untuk melakukan transaksi yang berikutnya. Hal ini untuk menghindari penyalahgunaan oleh pihak yang tidak bertanggung jawab.

- **Tahap otentikasi kunci dan pengguna pada server**
  Setelah kode pembangkitan kunci dikirimkan kepada *client*, pada sisi *server* akan dilakukan penyimpanan kode dan pengguna yang memiliki kode tersebut. Tahap ini digunakan sebagai proses otentikasi pengguna *mobile banking* selama sesi komunikasi berlangsung.
  Selain itu juga, server akan melakukan pembangkitan kunci sesuai dengan parameter kode yang dikirimkan kepada *client*. Skema otentikasi user bisa diilustrasikan pada gambar 6.



Gambar 6 : Skema Otentikasi *client*

- **Tahap transaksi data**
  Pada tahap ini *client* yang hendak melakukan komunikasi dengan server harus memiliki kunci (*session key*) yaitu sebuah kunci yang hanya bisa digunakan pada saat sesi tersebut berlangsung. *Client* yang telah memiliki *session key* akan melakukan proses enkripsi pada pesan menggunakan kunci yang sudah dibangkitkan tersebut.
  Pesan yang dikirim melalui jaringan publik (internet) berupa pesan *ciphertext* yang aman. Model pengamanan dengan skema komunikasi *client server* ini bisa terlihat seperti gambar 7.



Gambar 7 : Proses transaksi pesan *mobile banking*.

Berdasarkan gambar 6 di atas, dapat dideskripsikan bahwa transaksi pesan dalam sistem mobile banking ini menggunakan format *ciphertext*. Ketika pesan *ciphertext* sampai ke server, maka pesan akan didekripsikan menggunakan kunci *session key* yang dimiliki oleh *server*. Sebuah pesan *ciphertext* hanya bisa didekripsikan jika kunci enkripsi dan dekripsinya sama. Pada penelitian ini, pemilihan panjang kunci untuk digunakan pada perangkat *mobile* juga menjadi perhatian.

Algoritma pengamanan

Untuk proses pengamanan pesan dalam transaksi mobile banking, skema algoritma yang digunakan antara lain:

- **Algoritma Pembangkitan kunci (Generating)**
  Algoritma *Generating* digunakan untuk membentuk kunci yang akan digunakan untuk proses komunikasi antara *client* dan *server*. Kunci yang dibangkitkan berasal dari random *key* yang diberikan oleh *server*. Algoritma pembangkitan kunci bisa dideskripsikan pada gambar 8.

```
KeyGenerator kgen=KeyGenerator.getInstance("AES");
//Pemilihan Kode Random
SecureRandom
sr=SecureRandom.getInstance("SHA1PRNG");
kgen.init(128,sr);
  SecretKey skey=kgen.generateKey();
```

Gambar 8 : Algortima pembangkitan kunci

- **Algoritma Enkripsi**

Algoritma enkripsi digunakan sebagai bentuk pengamanan akan diterapkan dalam pengubahan bentuk *plaintext* menjadi *ciphertext*. Algoritma enkripsi ini bisa diilustrasikan pada gambar 9.

```
Mulai
// Pemilihan cipher
Cipher cipher =
Cipher.getInstance("AES/CBC/PKCS5Padding");
//Pemilihan Kunci
SecretKeySpec key = new
SecretKeySpec(enc_key,AES");
cipher.init(Cipher.ENCRYPT_MODE, key,new
IvParameterSpec(iv));
return cipher.doFinal(plainText.getBytes());
Selesai
```

Gambar 9 : Algortima enkripsi pesan

- **Algoritma Dekripsi**

Algoritma dekripsi ini digunakan untuk membuka pesan *ciphertext* yang sudah melalui proses enkrispi menggunakan algoritma enkripsi sebelumnya. Algoritma enkripsi ini bisa diilustrasikan pada gambar 10.

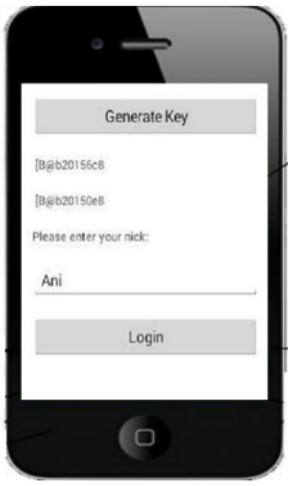
```
Mulai

//Pemiliihan cipher
Cipher cipher= Cipher.getInstance("AES/CBC/PKCS
5Padding");
//Pemilihan kunci dekripsi
SecretKeySpec key = new SecretKeySpec(enk_key,
"AES");
cipher.init(Cipher.DECRYPT_MODE, key,new IvPara
meterSpec(iv));
//Hasil
return new String(cipher.doFinal(cipherText));

Selesai
```

Gambar 10 : Algortima dekripsi pesan

Untuk meningkatkan aspek keamanan pesan yang dikirim melalui jaringan publik, pemilihan parameter untuk algoritma dekripsi menjadi sangat penting.

2. Pembahasan

Hasil percobaan yang dilakukukan menunjukkan proses pembangkitan kunci, enkripsi dan dekripsi pesan membutuhkan waktu yang cukup singkat. Proses pembangkitan kunci bisa dilihat pada gambar 11.



. Gambar 11 : Proses pembangkitan kunci

Dalam melakukan pengamanan pesan *mobile banking*, beberapa teknik dilakukan pada parameter pembentuk kunci dan proses enkripsi/dekripsi. Pemilihan parameter pengamanan sangat menentukan tingkat keamanan sebuah pesan yang ditransmisikan melalui jaringan publik. Penelitian ini menerapkan beberapa parameter pengamanan pesan beserta analisanya.

Keamanan *Random Number*

Ada dua teknik yang umumnya digunakan untuk membangkitkan *random bit* yaitu teknik pembangkitan *deterministic* yang mana operasi pembangkitan berdasarkan pada proses fisik yang terjadi dan *non-deterministic* yang mana operasi perhitngan *random number* berdasarkan pada algortima yang disebut sebagai *Deterministic Random Bit Generators (DRBGs).*
DRBG merupakan teknik pembangkitan *Random Number* yang bisa digunakan untuk proses pembangkitan *random bit* yang digunakan pada perhitungan kriptografi (Barker, Kelsey, 2012)
Pada penelitian ini, digunakan skema DRBG yang akan diterapkan pada algoritma *Advanced Encryption Standard* (AES) yang diterapkan pada proses komunikasi *mobile banking*, teknik pemilihan *secure random* sangat penting untuk keamanan pesan yang akan dienkripsi. Pada penelitian pembangkitan *Random Number* akan menggunakan teknik *Deterministic Random Bit Generators* (DRBG).

Teknik Pengamanan *Initialization Vektor* (IV)

Algoritma AES merupakan sebuah algoritma dengan model kerja berbasis *block cipher*. Algoritma AES umum menggunakan mode operasi *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB) dan *Output Feedback* (OFB) untuk menghasilkan nilai *Initialization Vektor* (IV) sebagai inputan. Pemilihan mode operasi pada algoritma *block cipheri* sangat penting

dalam mengukur kualitas keamanan dan tingkat komputasi sebuah algortima (M. Dworkin, 2001)
Nilai IV merupakan komponen yang harus dibangkitkan pada saat proses enkripsi dan dekripsi pesan, sehingga IV mestinya memiliki skema pengamanan tersendiri dalam proses komunikasi dua arah *mobile banking*. Pada mode CBC (R. J. Easter, 2012)
Pada penelitian ini, proses untuk menentukan *Initialization Vektor* (IV) akan menggunakan teknik *random number* yang sesuai dengan rekomendasi FIPS terbaru pemilihan teknik pengamanan IV akan meningkatkan keamanan pesan *plaintext* dan *ciphertext* pada proses transaksi data jika diterapkan pada aplikasi *mobile banking*.

Kecepatan komputasi AES

Algoritma AES memiliki tingkat keamanan yang baik dalam proses pengamanan data dan sangat banyak digunakan dalam pengamanan aplikasi komputer saat ini. Tetapi, proses komputasi pada algoritma AES menggunakan *memory* komputer yang cukup besar. Hal ini kurang cocok dengan sumber daya yang dimiliki oleh perangkat *mobile.* Oleh karena itu, pemilihan table round menjadi solusi untuk mengurangi kebutuhan *resource* pada proses komputasi (X.-Q. Luo, 2015).
Pada penelitian ini, diterapkan skema penentuan jumlah batasan *table round* untuk penerapan pada mobile banking. Pemilihan *table round* yang cocok pada perangkat *mobile* menjadi pilihan utama disamping memperhatikan aspek keamanan berbasis *random number* dan *Initialization Vektor*.

3. Kesimpulan

Aspek keamanan transaksi pada *mobile banking* saat ini membutuhkan metode pengamanan yang baik dan memiliki tingkat komputasi yang efisien. Pada penelitian ini, sebuah metode pengamanan pesan *mobile banking* menggunakan algoritma *Advanced Encryption Standard* (AES) .

Tingkat keamanan pesan dan efisiensi komputasi pada *mobile banking* ditentukan oleh pemilihan beberapa aspek yaitu: *Random Number, Initialization Vektor* (IV), Kecepatan komputasi AES.

Pada penelitian ini, digunakan skema DRBG yang akan diterapkan pada algoritma *Advanced Encryption Standard* (AES) yang diterapkan pada proses komunikasi *mobile banking*, teknik pemilihan *secure random.* Pada penelitian ini, proses untuk menentukan *Initialization Vektor* (IV) menggunakan teknik *random number* yang sesuai dengan rekomendasi FIPS terbaru pemilihan teknik pengamanan IV akan meningkatkan keamanan pesan *plaintext* dan *ciphertext* pada proses transaksi data jika diterapkan pada aplikasi *mobile banking*. Efisiensi komputasi dengan algoritma AES akan tercapai jika pemilihan *table round* tidak melebihi ukuran 512.

Daftar Pustaka

[1] K.-H. Shih and C.-Y. Lin, “Is mobile banking a competitive weapon?,” *Int. J. Electron. Finance*, vol. 8, no. 2–4, pp. 189–201, 2015
[2] X.-Q. Luo, Y. Qi, Y.-D. Wan, and Q. Wang, “Low-cost and fast AES encryption method for industrial wireless network,” *Beijing Youdian Daxue XuebaoJournal Beijing Univ. Posts Telecommun.*, vol. 38, no. 1, pp. 55–60, 2015.
[3] R.L. Rivest, A. Shamir, L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Massachusetts Institute of Technology, Cambridge, 1994
[4] P. Faruki, A. Bharmal, V. Laxmi, V. Ganmoor, M. S. Gaur, M. Conti, and M. Rajarajan, “Android security: A survey of issues, malware penetration, and defenses,” *IEEE Commun. Surv. Tutor.*, vol. 17, no. 2, pp. 998–1022, 2015.
[5] C. Lupu, V.-G. Gəitan, and V. Lupu, “Security enhancement of internet banking applications by using multimodal biometrics,” presented at the SAMI 2015 - IEEE 13th International Symposium on Applied Machine Intelligence and Informatics, Proceedings, 2015, pp. 47–52.
[6] Kus Ikhsanto, Ifadah Amalia, ANALISIS KEAMANAN INTERNET BANKING PADA BANK DI INDONESIA Sistem Informasi, Fakultas I1mu Komputer, Universitas Gunadarma, 2012
[7] Budiono, PENERAPAN TANDA TANGAN DIGITAL UNTUK KEAMANAN TRANSAKSI SMS – BANKING, 2013.
[8] FIPS, "Announcing the ADVANCED ENCRYPTION STANDARD(AES)*“Information Technology Laboratory, National Institute of Standards and Technology (NIST).*2001.
[9] E. Barker and J. Kelsey, "Recommendation for Random Number Generation Using Deterministic Random Bit Generators *“Information Technology Laboratory, National Institute of Standards and Technology* (NIST).2012
[10] R. J. Easter, “Approved Random Number Generators for FIPS PUB 140-2, Security Requirements for Cryptographic Modules”, National Institute of Standards and Technology (NIST), 2012.
[11] M. Dworkin, “Recommendation for Block Cipher Modes of Operation”, National Institute of Standards and Technology (NIST), 2001.
[12] J. Daemen and V. Rijmen, “AES proposal: Rijndael”, First Advanced Encryption Standard (AES) Conference, (1998).
[13] J. Viega, M. Messier and P. Chandra, “Network Security with OpenSSL: Cryptography for Secure Communications”, O'Reilly Media, Inc., (2002).
[14] IEEE Standards Association, 802.11-2012-IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, (2012).
[15] Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LRWPANs), IEEE Computer Society Std. 802.15.4, (2007).

[16] Vasco, Security: a major concern for the adoption of m-banking. 2009.
[17] B. Singh and K. S. Jasmine, *Secure end-to-end authentication for mobile banking*, vol. 349. 2015.
[18] Stallings,W,, Cryptography and Network Security , ". Prentice Hall, 2006
[19] Menezes A., Van Oorschot P, & Vanstone S. "Handbook of Applied Cryptography". *CRC Press Inc*. 1996.
[20] Forouzan, A Behrouz. "Cryptography and Network Security. Singapore," *Mc Graw-Hill Education (Asia)*, 2008
[21] Scheiner B. "Applied Cryptography Protocols, Algorithms and Source Code in C. Second Edition." New York: *John Wiley & Sons,inc*, 1996.
[22] K. Rahimunnisa, P. Karthigaikumar and J. Kirubavathy, "A 0.13-µm implementation of 5 Gb/s and 3-mW folded parallel architecture for AES algorithm", International Journal of Electronics, vol. 1-12, (2013).
[23] S. Morioka and A. Satoh, "A 10-Gbps full-AES crypto design with a twisted BDD S-Box architecture", IEEE Transactions on VLSI Systems, vol. 12, no. 7, (2004), pp. 686-691.
[24] Q. Yue, L. Xinqiang, and W. Yadong, "Low-cost round encryption method for embedded system," *Int. J. Secur. Its Appl.*, vol. 9, no. 4, pp. 117–124, 2015
[25] G. Bertoni, L. Breveglieri and P. Fragneto, "Efficient software implementation of AES on 32-bit platforms", Cryptographic Hardware and Embedded Systems-CHES, (2003), pp. 159-171.
[26] B. Gladman, "A Specification for Rijndael, the AES Algorithm", Available at http://fp.gladman.plus.com, (2002).
[27] K. Atasu, L. Breveglieri and M. Macchetti, "Efficient AES implementations for ARM based platforms", Proceedings of the ACM symposium on Applied computing, ACM, (2004); Nicosia, Cyprus.

Biodata Penulis

Putra Wanda, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika Universitas Respati Yogyakarta, lulus tahun 2011. Memperoleh gelar Master of Engineering(M.Eng) Program Pasca Sarjana Magister Teknologi Informasi Universitas Gajah Mada Yogyakarta, lulus tahun 2015.Saat ini menjadi Dosen di Universitas Respati Yogyakarta.

ISSN : 2302-3805