Aplikasi Kriptografi Untuk Keamanan Pelaporan Pemungutan Suara Pada Pemilihan Umum Presiden Berbasiskan Layanan Pesan Pendek di Indonesia

Puja Pramudya

Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung
Jl. Cisitu Lama 3D/160B, Bandung, Jawa Barat
e-mail: puja.pramudya@gmail.com
if16058@students.if.itb.ac.id

Abstrak- *Short Message Service (SMS) merupakan suatu pesan yang dapat diterima dan dikirimkan oleh ponsel melalui layanan operator seluler tertentu, baik bersifat CDMA maupun GSM.Pelaporan hasil pemungutan suara pemilihan presiden di Indonesia akan menggunakan sistem pelaporan cepat melalui layanan pesan pendek (SMS) yang sudah diterapkan berbagai lembaga survey melalui sistem quick count. Dengan sistem ini diharapkan rekapitulasi suara dapat dilakukan dengan cepat,akurat dan efisien. Faktor keamanan menjadi sangat penting untuk mendukung sistem pelaporan tersebut dikarenakan untuk sistem pelaporan suara ini dibutuhkan keakuratan dan keabsahan data yang sangat tinggi. Aplikasi kriptografi dengan menggunakan tanda tangan digital pada isi laporan mampu meningkatkan level keamanan dengan menggunakan prinsip hashing dan kriptografi kunci publik. Dengan menggunakan tanda tangan digital maka proses pembentukan tanda tangan dari pesan yang akan dikirim dan proses pemeriksaan keabsahannya dapat dilakukan sehingga otentikasi pengirim dan integritas data dapat terjamin sekaligus.*

Kata Kunci *: Tanda tangan digital, hashing, kriptografi kunci publik*

1. Pendahuluan

Pemilihan umum presiden merupakan pesta demokrasi lima tahunan yang dilaksanakan di Indonesia untuk memilih pemimpin negara yang akan mengabdi dalam rangka mewujudkan Indonesia yang makmur dan sejahtera bagi seluruh rakyat di tanah air. KPU (Komisi Pemilihan Umum) sebagai lembaga yang bertanggungjawab terhadap pelaksaan pemilu tentu harus mampu menyediakan infrastruktur yang aman untuk mendukung terlaksananya pemilu agar dapat berlangsung dengan baik, valid dan akuntabel.

Pada pemilihan umum ini terdapat kebutuhan untuk melaporkan hasil pemungutan suara di TPS-TPS yang tersebar di seluruh tanah air dengan cepat tanpa mengurangi akurasi dan validitas laporan. Transformasi teknologi informasi memiliki dampak yang signifikan dalam infrastruktur pendukung pemilihan umum presiden. Saat ini, KPU sedang menyiapkan sistem pelaporan hasil pemungutan suara dalam Pemilu Presiden melalui *short messages service* (SMS). Teknologi berbasiskan layanan pesan pendek ini lebih memungkinkan digunakan pada pemilu presiden daripada pemilu legislatif karena variasi data untuk pemilihannya relatif lebih sedikit.

Penggunaan SMS untuk pelaporan suara sudah sangat populer digunakan oleh lembaga survey untuk mendukung perhitungan *quick count* pemilu legislatif di Indonesia . Dalam hal ini faktor keamanan tentu menjadi sangat penting dikarenakan data yang ingin dikirimkan sifatnya sangat sensitif dan harus terjamin kebenarannya. Tentu bukan SMS dari sembarang ponsel yang digunakan. SMS yang akan diproses oleh sistem hanyalah SMS dari ponsel yang nomornya terdaftar di dalam sistem.

Dengan sistem tersebut terdapat beberapa celah keamanan yang mungkin dapat dimanfaatkan orang-orang tidak bertanggungjawab. Misalnya apabila ponsel petugas hilang dan digunakan oleh orang tertentu yang mengetahui format isi laporan atau apabila ditengah transmisi isi pesan dapat diambil oleh orang yang tidak berwenang. Salah satu cara untuk menanggulangi hal tersebut adalah mengaplikasikan kriptografi dalam sistem pelaporan pemungutan suara pemilihan umum presiden di Indonesia.

2. Tinjauan Pustaka

2.1. Pelaporan Hasil Pemungutan Suara

2.1.1. Sistem KPU

Sistem penghitungan suara elektronis KPU untuk pemilu legislatif menggunakan teknologi ICR atau

Intelligent Character Recognition. ICR adalah adalah teknologi yang mengandalkan intelegensi buatan untuk mengenali tulisan tangan menjadi data. ICR diyakini sulit mencapai akurasi 98%, kecuali jika tesnya sangat terbatas dan kondisinya terekayasa dengan apik. Tulisan tangan setiap orang berbeda-beda. Tulisan tangan orang yang sama pun berbeda-beda. Kadang suatu ketika menulis agak miring ke kanan, kadang miring ke kiri kadang tegak. ICR akan berusaha sebaik mungkin untuk ***menebak*** tulisan tangan yang dibaca berdasarkan kemiripan atas kriteria-kriteria tertentu yang diterapkan pada algoritma yang digunakan. ICR bertumpu pada cara atau algoritma yang digunakan dalam menebak. Yang namanya tebakan, semakin sering menebak makin banyak benar dalam tebakannya, dan setiap tebakan bisa diperkirakan tingkat keyakinan akan benar tidaknya tebakan tersebut.

Hal ini adalah salah satu kekurangan dari teknologi ICR yaitu pada saat dia **yakin** tebakannya **benar** tapi ternyata **salah** atau yang disebut sebagai "False Positive". Karena false positive ini tidak bisa dihindari, maka **tidak ada satu lembar pun hasil scanning yang tidak perlu diverifikasi dan divalidasi**, berapapun tingginya akurasi yang diklaim oleh sebuah produk ICR. Inilah jebakan yang harus dihindari jika **akurasi** dari data adalah segalanya, dan karenanya secara teknis sebenarnya ICR tidak cocok digunakan untuk penghitungan suara yang harus **akurat** dan **cepat**.

2.1.2. Sistem Quick Count

Pelaporan hasil pemungutan suara merupakan bagian penting dalam proses penghitungan suara. Saat ini, *Quick Count*, yang menjadi pusat perhatian seluruh masyarakat yang ingin memantau hasil perhitungan suara secara instan menggunakan teknologi SMS untuk mendukung pengumpulan data.

Secara umum skema survey *quick count* dilakukan oleh petugas lapangan lembaga yang bertugas dengan mengirimkan SMS berisi hasil rekap suara ke SMS *server*. SMS yang masuk ke *server* hanya akan dibaca bila SMS tersebut berasal dari nomor yang telah terdaftar. Bila SMS berasal dari nomor lain, hasilnya tidak akan mempengaruhi perhitungan *quick count*.

Ketika data SMS sampai di *server* , pesan akan divalidasi secara otomatis, mulai dari nomor, isi, dan kemudian dibandingkan dengan data yang tersimpan di *database*. Bila *database* ternyata telah menyimpan data yang dikirim dari entri manual terlebih dahulu maka data dari SMS tidak akan digunakan. Begitu pula data SMS yang masuk gagal karena dikirim dengan format penulisan yang salah maka sistem akan menggunakan data dari entri manual.

Gambar 1 Skema Pelaporan Pemungutan Suara Via SMS

2.2. Penggunaan SMS Untuk Sistem Pelaporan Hasil Pemungutan Suara Presiden

Berbeda dengan pemilu legislatif yang menggunakan sistem ICR, Komisi Pemilihan Umum sedang menyiapkan sistem pelaporan hasil pemungutan suara dalam Pemilu Presiden melalui *short messages service* (SMS). Teknologi SMS lebih memungkinkan digunakan di Pemilu Presiden daripada di Pemilu legislatif karena variasi datanya lebih sedikit. Dari satu partai saja terdapat calon untuk Dewan Perwakilan Rakyat, Dewan Perwakilan Daerah dan Dewan Perwakilan Rakyat Daerah sehingga kompleksitas cukup tinggi dan dikhawatirkan sangat berpotensi terjadi kesalahan entri data.

Sistem ini sedang dalam masa pengujian. Pengiriman data melalui SMS ini diharapkan akan menjadi lebih cepat. Untuk otentifikasi, KPU merancang sistem pengidentifikasian nomor pengirim apakah sudah terdaftar dan berasal dari TPS tertentu.

SMS digunakan karena teknologi itu memberikan hasil suara yang cepat. SMS dapat mempersingkat jeda waktu yang banyak terbuang bila dilakukan lewat telepon atau pemindaian menggunakan ICR. SMS dapat memotong jalur penyampaian data dari hulu ke hilir secara efisien. Selain itu, SMS adalah teknologi yang mudah, telah diakses luas oleh banyak orang serta proses *coding* yang relatif mudah.

3. Desain Keamanan Sistem Pelaporan Hasil Pemungutan Suara Presiden

Berdasarkan paparan di atas, sistem pelaporan hasil pemungutan suara presiden yang sekarang sedang dirancang memiliki karakteristik sebagai berikut :

- Otentikasi pengirim laporan menggunakan nomor ponsel yang terdaftar pada sistem
- Isi laporan dikirimkan tanpa pemrosesan lebih lanjut

Dengan sistem seperti ini terdapat beberapa celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggungjawab. Beberapa celah tersebut adalah :

- Apabila ponsel petugas resmi dicuri oleh orang lain dan pencuri mengetahui format laporan yang digunakan KPU maka pencuri dapat mengirimkan laporan ke sistem. Dikarenakan nomor petugas resmi terdaftar maka laporan akan dianggap valid.
- Apabila laporan dikirimkan melalui jaringan dan ditengah jaringan terdapat orang yang melakukan penyadapan dan mengubah isi laporan maka hasil laporan dapat dianggap valid oleh sistem.

Mengingat laporan pemungutan suara melalui SMS harus tetap menjaga kecepatan dan keakuratan data maka perlu didesain sistem keamanan yang dapat memastikan laporan yang diterima oleh sistem merupakan laporan yang benar, sah dan valid. Untuk itu tentu saja diperlukan modifikasi dari sistem yang sedang dirancang oleh KPU. Berikut penulis akan mengusulkan desain keamanan untuk sistem pelaporan pemungutan suara presiden berbasiskan layanan pesan pendek dengan menggunakan prinsip-prinsip kriptografi.

3.1. Protokol Pengiriman Laporan Pemungutan Suara

Skema yang diusulkan untuk dapat meningkatkan keamanan dalam pengiriman laporan pemungutan suara menggunakan prinsip kriptografi adalah :

Komunikasi Tanda Tangan Digital

Prinsip komunikasi ini menggunakan tanda tangan digital untuk menjamin integritas data dan otentikasi. Lebih lengkapnya desain komunikasi dengan tanda tangan digital adalah sebagai beriku t:

1. Pelapor memberi tanda tangan digital pada *message digest* pesan laporan dengan fungsi *hash*
2. Pelapor mengenkripsi *message digest* laporan dengan kunci privat pelapor. Hasil enkripsi dilekatkan pada pesan laporan
3. Pelapor mengirim pesan laporan bersama dengan *digital signature*
4. KPU meringkas pesan laporan menjadi *message digest* dengan fungsi *hash* yang sama
5. KPU mendekripsi tanda tangan digital dengan kunci publik pada basis data yang disertakan dalam pesan laporan
6. KPU membandingkan *message digest* yang dihasilkan dengan dekripsi dari tanda tangan digital, jika sah maka pesan laporan dapat digunakan

3.2. Fungsi *Hash* Satu-Arah

Untuk implementasi yang lebih sederhana tanpa mengurangi tingkat keamanan pelaporan pengiriman suara maka penggunakan komunikasi tanda tangan digital lebih disarankan. Proses menghasilkan tanda tangan digital dari isi laporan, akan menggunakan fungsi *hash* satu arah.

Fungsi *hash* adalah fungsi yang menerima masukan *string* yang panjangnya sembarang dan mengkonversinya menjadi string keluaran yang panjangnya tetap (*fixed)*. Fungsi *hash* mengkompresi sembarang pesan yang berukuran berapa saja menjadi *message digest* yang ukurannya selalu tetap. Fungsi *hash* satu-arah (*One-way hash*) adalah fungsi *hash* yang bekerja dalam satu arah :pesan yang sudah diubah menjadi *message digest* tidak dapat dikembalikan lagi menjadi pesan semula. Dua pesan yang berbeda akan selalu menghasilkan nilai *hash* yang berbeda pula.

Fungsi *hash* satu-arah yang dapat digunakan pada sistem adalah MD5. MD5 adalah fungsi *hash* yang dibuat oleh Ronald Rivest pada tahun 1991. MD5 menerima masukan berupa pesan denga nukuran sembarang dan menghasilkan *message digest* yang panjangnya 128 bit. Langkah-langkah pembuatan *message digest* secara garis besar adalah sebagai berikut :

1. Penambahan bit-bit pengganjal (*padding bits*)
2. Penambahan nilai panjang pesan semula
3. Inisialisasi penyangga *buffer* MD
4. Pengolahan pesan dalam blok berukuran 512-bit

3.3. Algoritma RSA

Untuk kekuatan pengiriman pesan, *message digest* akan dienkripsi dengan algoritma RSA, salah satu kriptografi kunci publik yang populer. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan kunci privat. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin.

RSA menggunakan kunci berbeda untuk enkripsi dan dekripsi. Untuk pembangkitan kunci menggunakan algoritma berikut :

1. Pilih dua buah bilangan prima sembarang, p dan q
2. Hitung $n = p.q$ (sebaiknya p tidak sama dengan q)
3. Hitung $\emptyset(n) = (p-1)(q-1)$
4. Pilih kunci publik, e, yang relatif prima dengan $\emptyset(n)$
5. Bangkitkan kunci privat dengan menggunakan persamaan $d = \frac{1+k\emptyset(n)}{e}$

Hasil dari algoritma di atas adalah :

- Kunci publik adalah pasangan (e,n)
- Kunci privat adalah pasangan (d,n)

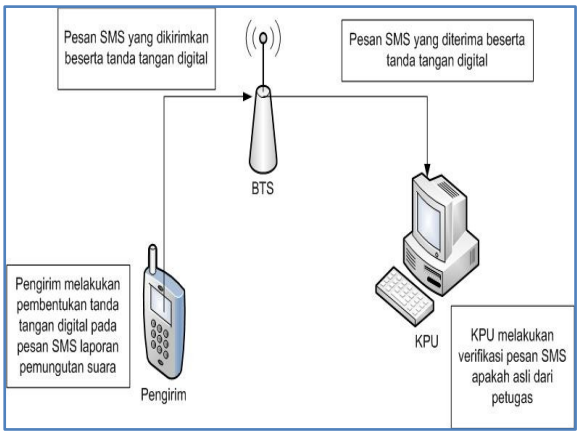
Untuk algortima enkripsi dan dekripsi menggunakan RSA adalah :

Enkripsi
Ambil kunci publik penerima pesan,e dan modulus n
Nyatakan plainteks m menjadi blok-blok $m_1, m_2, \ldots$, sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang [0,n-1]

Setiap blok m_i dienkripsi menjadi blok c_i dengan rumus $c_i = m_i^{\ d} \bmod n$

Dekripsi
Setiap blok cipherteks c, didekripsi kembali menjadi blok mi dengan rumus $m_i = c_i^{\ d} \bmod n$

3.4. Arsitektur Tanda Tangan Digital SMS Sistem Pelaporan Hasil Pemungutan Suara



Gambar 2 Arsitektur Sistem Pelaporan Pemungutan Suara

Gambar diatas menunjukkan arsitektur rancangan sistem pelaporan hasil pemungutan suara presiden pada sistem KPU. Terdapat aplikasi yang akan dibangun pada ponsel petugas, untuk memberikan tanda tangan digital pada SMS laporan. Pada sisi server, terdapat aplikasi untuk
menverifikasi data SMS yang masuk. Implementasi pada sisi server dapat berupa penambahan modul dari aplikasi yang sudah ada karena kebutuhan utama adalah verifikasi tandatangan digital pada pesan yang dapat dilakukan dengan menambahkan beberapa fungsi.

Seluruh laporan pemungutan suara nantinya akan dikirimkan menggunakan tanda tangan digital SMS. Tanda tangan digital SMS merupakan tanda tangan digital pada pesan SMS yang merupakan nilai kriptografis dengan menggunakan prinsip-prinsip pada bidang ilmu kriptografi. Tanda tangan digital ini selalu berbeda-beda antara satu isi pesan SMS laporan dengan pesan SMS lain.

Standar yang digunakan untuk pembentukan tandatangan digital adalah :

- Fungsi *hash* MD5
- Algoritma kunci publik RSA untuk enkripsi *message digest*

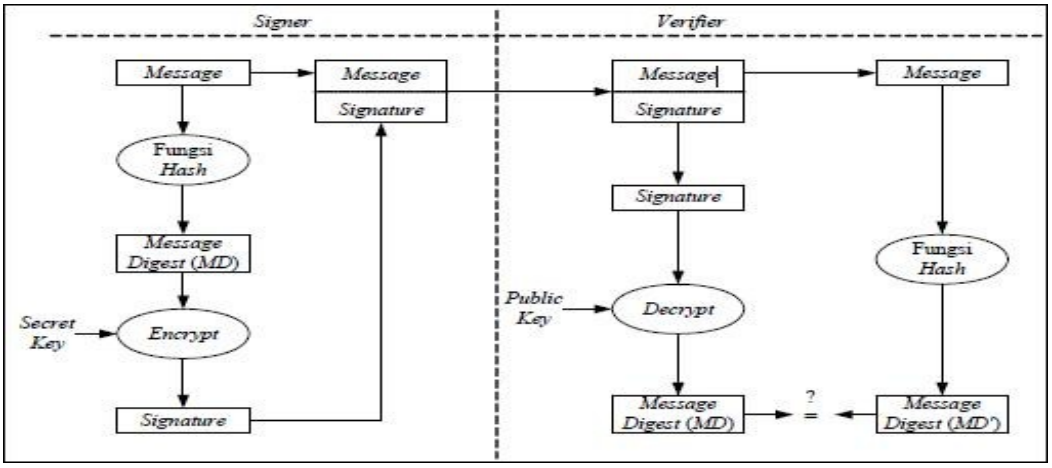
Pada sistem harus diimplementasikan dua kebutuhan berikut :

1. Pembentukan tanda tangan digital yaitu dengan menggunakan kunci rahasia (kunci yang hanya diketahui oleh penerima pesan)
2. Pemeriksaan keabsahan tandatangan digital dengan menggunakan kunci publik yang berpadanan.

Setiap pesan SMS yang akan dikirim akan diubah menjadi *message digest* (MD) dengan menggunakan fungsi MD5. Setelah itu akan dilakukan proses enkripsi untuk membentuk tandatangan digital dengan menggunakan kunci privat yang hanya diketahui oleh pengirim. Tandatangan digital yang terbentuk tersebut akan dikirimkan beserta dengan pesan SMS.

Pesan SMS yang diterima diverifikasi dengan mengambil bagian tandatangan digitalnya lalu mendekripsi tanda tangan tersebut dengan kiunci publik yang diketahui oleh KPU. Tanda tangan digital yang didekripsi akan menghasilkan MD yang kemudian dicocokkan dengan hasil *hash* dari pesan

SMS. Jika MD menunjukkan kesamaan maka pesan SMS itu memang dikirimkan dari petugas resmi KPU dan integritas datanya terjamin sehingga dapat digunakan untuk keperluan selanjutnya.



Gambar 3 Skema Tanda Tangan Digital

4. Implementasi Tanda Tangan Digital SMS pada *Windows Mobile*

Untuk implementasi prototipe aplikasi tanda tangan digital SMS pada perangkat *mobile*, penulis akan menggunakan *framework* Microsoft .NET 3.5 CF pada Windows Mobile 6 dengan bahasa C#. Adapun kebutuhan kelas didefinisikan sebagai berikut:

Tabel 1 Kebutuhan Kelas Implementasi

No	Kelas	Fungsi
1	MD5	*Wrapper class* untuk fungsi MD5 .NET
2	BigInt	Kelas implementasi bilangan bulat besar yang dibutuhkan untuk parameter RSA
3	RSACrypter	Kelas implementasi algoritma RSA
4	myForm	Kelas untuk antarmuka dan program utama

Skenario pembentukan tanda tangan digital dengan program aplikasi ini mengasumsikan petugas KPU / TPS telah mengetahui kunci privat yang berpadanan dengan kunci publik yang dimiliki KPU dan format laporan telah disepakati kedua belah pihak. Tanda tangan digital akan ditambahkan pada bagian akhir pesan laporan dengan format `<ds><tanda_tangan></ds>`.

Skenario pembubuhan tanda tangan digital lebih lengkap dijelaskan sebagai berikut :

1. Pelapor memasukkan nomor yang akan dituju (dalam hal ini adalah SMS server milik KPU)
2. Pelapor memasukkan isi laporan hasil pemungutan suara

Gambar 4 Tampilan Input Nomor Tujuan dan Isi Laporan

3. Pelapor memilih menu *Input Key*
4. Pelapor memasukkan nilai kunci privat dan parameter N

Gambar 5 Tampilan Input Pasangan Kunci

5. Pelapor memilih menu *Add Signature* (proses pembubuhan tanda tangan digital)

Gambar 6 Tampilan Hasil Tanda Tangan Digital

Kode implementasi pembubuhan tanda tangan digital adalah sebagai berikut :

```
/// <summary.
/// menambahkan signature pada pesan
/// </summary>
/// <param name="sender"></param>
/// <param name="e"></param>
private void myAddSign_Click(object sender,
EventArgs e)
        {
MD5 md = new MD5();
RSACrypter rs = new RSACrypter();

string s = md.getHash(myTextField.Text);
rs.init(md.DecimalString, new
BigInt("105611", 10), new
BigInt(privKeyField.Text, 10) , new
BigInt(paramNField.Text, 10) );
myTextField.Text += "<ds>" +
rs.getDigi(rs.blockRSA) + "</ds>";
this.Focus();
}
```

6. Pelapor mengirimkan pesan

Kode implementasi pengiriman pesan adalah sebagai berikut :

```
private void send_Click(object sender,
EventArgs e)
 if
(myDestinationField.Text.Equals(String.Empty)
|| myDestinationField.Text.Length < 8)
 {
    errMessage.Text = "Error!";
 }
 else
 {
    SmsMessage OutgoingMessage = new
SmsMessage(myDestinationField.Text,
myTextField.Text);
    OutgoingMessage.Send()
  }
}
```

5. Kesimpulan

Dari analisa yang didapatkan dari hasil implementasi dapat dsimpulkan bahwa tanda tangan digital terhadap pesan dapat dilakukan terhadap pesan SMS melalui perangkat seluler. Untuk itu, hal ini sangat baik diterapkan dalam proses pelaporan pemungutan suara pemilihan presiden di Indonesia karena meningkatkan level keamanan rekapitulasi suara menjadi dua level, yaitu:

1. Autentikasi laporan berdasarkan nomor pelapor (terdaftar pada sistem)
2. Validasi menggunakan tandatangan digital yang terdapat pada pesan laporan

Aplikasi kriptografi menggunakan tanda tangan digital akan mampu menangani dua permasalahan keamanan sebagai berikut :

1. Orang tidak bertanggungjawab melaporkan hasil suara menggunakan ponsel petugas resmi
2. Pada proses pengiriman, orang tidak bertanggungjawab mengubah isi pesan laporan

Tentu saja yang tidak kalah pentingnya adalah pengaturan manajemen kunci dan distribusi pasangan kunci petugas-KPU sehingga protokol keamanan ini dapat berjalan dengan baik.

Secara garis besar tulisan ini telah mampu membuktikan penerapan tanda tangan digital untuk keamanan pelaporan hasil pemungutan suara pemilihan presiden menggunakan layanan pesan pendek (SMS) melalui aplikasi kriptografi, yaitu penggunaan fungsi MD5 dan RSA yang cukup sederhana. Selanjutnya, sebaiknya dipilih platform yang lebih umum sehingga dapat digunakan secara luas terhadap ponsel yang digunakan pada lingkup petugas KPU.

Daftar Pustaka

[1] Munir, Rinaldi, Diktat Kuliah IF5054 Kriptografi, Penerbit ITB 2006

[2]http://ardh1net.blogdetik.com/readblog/2009/04/15/211058/736/publikasi-ip-server-vpn-kpu-picu-penyusupan-hacker

[3]http://politik.vivanews.com/news/read/48703-laporan_hasil_pemilu_presiden_pakai_sms

[4]http://geeks.netindonesia.net/blogs/tahir/archive/2009/03/16/teknologi-apa-yang-baru-pada-sistem-ti-pemilu-2009.aspx