MODEL DATABASE WEB E-PILKADA BERBASIS KRIPTOGRAFI FUNGSI HASH

Muslim[1)], Dolly Indra[2)]
[1] Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia, Makassar
E-mail: mus_lim2003@yahoo.com
[2] Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia, Makassar
E-mail: dolly_indra2002@yahoo.com

Abstrak

*Dibalik perkembangan teknologi web yang begitu cepat dan semakin canggih, kriminal dalam bidang ini juga sangat maju dan terus meningkat, seperti sering terjadi di Indonesia, **attacker** menyerang berbagai situs pemerintah. Oleh karena itu, penelitian ini dimaksudkan untuk merancang "Model Database Web e-Pilkada berbasis Kriptografi Fungsi Hash" sehingga web pilkada dapat diakses dan aman terhadap praktek-praktek serangan dari pihak-pihak tidak bertanggungjawab. Pada model ini, unsur keamanan menggunakan fungsi hash MD5 dan fungsionalitas: login dua tahap, kontrol data sensitif secara periondik, dan **recovery** data. Model ini telah diuji pada prototipe situs KPU yang mengakses database pilkada. Hasilnya memperlihatkan bahwa data di dalam database aman, khususnya dalam aspek integritas.*

***Kata kunci*:** *Database web, e-Pilkada, Kriptografi Fungsi Hash, MD5.*

Abstract

*Behind the development of the web technology so rapidly and increasingly sophisticated, criminal in this field was also very advanced and continues to increase, like is often happens in Indonesia, attacker attacked various the government sites. Therefore, this research aims to design "e-Pilkada Web Database Model based Cryptographic Hash Function" so that the site pilkada is accessible and secure against attack practices by parties are not responsible. In this model, the security element using the Md5 hash function MD5 and functionalities: login two stages, control of sensitive data is periodically, and data **recovery**. This model has been tested on a prototype of the KPU site that accesses the e-Pilkada database. The results showed that the data in the database is safe, especially in the aspect of integrity.*

***Keywords*:** *Web Database, e-Pilkada, Cryptographic Hash Function, MD5.*

1. PENDAHULUAN

Data dan informasi di dalam database merupakan aset utama sebuah organisasi atau pemerintahan, misalnya database web pilkada. Dibalik perkembangan teknologi web yang begitu cepat dan semakin canggih, kriminal di bidang inipun juga tidak kalah majunya. Menurut statistik *cybercrime* terus meningkat (http://webappsec.org/projects/statistics), seperti kerap terjadi di Indonesia, *attacker* menyerang berbagai situs, misalnya situs KPU Indonesia pada tahun 2004 [1]. Hal ini memperlihatkan bahwa begitu rentangnya apalikasi berbasis web di Indonesia mendapatkan serangan dari orang tidak bertanggungjawab. Meskipun telah banyak usaha yang dilakukan untuk mencegah berbagai serangan dari orang tidak bertangungjawab [2][3][4][5]. Salah satu cara untuk mengatasi hal tersebut adalah dengan teknik kriptografi karena pada kriptografi terdapat sebuah fungsi yang cocok untuk keamanan informasi khususnya dalam aspek integritas informasi, yaitu fungsi hash misalnya MD5 [6][7]. Berdasarkan hal tersebut, maka penelitian ini dimaksudkan untuk merancang "Model Database Web e-Pilkada berbasis Kriptografi Fungsi Hash" sehingga dengan model ini aplikasi e-Pilkada dapat diakses dan aman dari praktek-praktek serangan oleh pihak tidak bertanggungjawab, mis. *Attacker*.

2. LANDASAN TEORI

2.1 Database Web

Database adalah sekumpulan data yang saling berhubungan dan terorganisir ke dalam *record-record* pada file-file dan disimpan secara bersama-sama sedemikian rupa untuk memenuhi berbagai kebutuhan [8], misalnya

database untuk Kepegawaian, Perbankan, Rumah Sakit, Kependudukan, Pilkada dan lain-lain. Sedangkan database yang diakses oleh aplikasi yang mendukung teknologi berbasis web disebut Database Web [9].

Untuk mengelola database secara fisik dilakukan oleh sebuah program sistem pengelola database atau DBMS (Data Base Management System), seperti MySql dan Microsoft Sql Server. Program DBMS ini akan menentukan bagaimana data diorganisir, disimpan, diubah dan diambil kembali. Dari kedua komponen tersebut dapat membentuk Sistem Database. Secara umum, sebuah sitem database merupakan sistem yang terdiri atas kumpulan file yang saling berhubungan dalam sebuah database di sebuah komputer dan seperangkat program yang memungkinkan pengguna dan aplikasi lain untuk mengakses dan memanipulasi file-file tersebut [8].

2.2 E-Pilkada

E-Pilkada adalah aplikasi komputer yang mendukung tugas-tugas institusi penyelenggara Pilkada di Indonesia. Aplikasi ini akan membuat proses-proses penyelenggaraan pilkada menjadi lebih efisien, transparan, dan akuntabel [10]. Dengan semakin luasnya jaringan komunikasi dan biaya komunikasi yang semakin murah, maka semakin terbuka peluang untuk diterapkannya teknologi web pada proses pemungutan, pengolahan dan perhitungan suara pilkada yang transparan dan akuntabel [11]. Teknologi berbasis web mempunyai kelebihan utama dalam hal kemudahan akses dan biaya yang jauh lebih murah [12]. Sehingga pemungutan suara secara elektronik dengan memanfaatkan teknologi informasi seperti e-Voting dan m-Voting yang saat ini dapat menjadi salah satu alternatif untuk menggantikan pemilihan umum secara konvensional yang sekarang ini digunakan [13]. Tersedianya fasilitas akses data secara luas, selain membuka peluang positif atas terapan berbagai aplikasi dan layanan berbasis internet, akan tetapi menyisakan persoalan terkait dengan keamanan data dan/atau informasi, khususnya dalam aspek integritas [14].

2.3 Fungsi Hash Kriptografi

Fungsi hash adalah suatu cara menciptakan *fingerprint* dari berbagai data masukan. Fungsi hash akan mentranspormasikan data untuk menciptakan *fingerprint*, yang biasa disebut nilai-hash. Nilai-hash biasanya digambarkan sebagai suatu string pendek yang terdiri atas huruf dan angka yang terlihat random (data biner yang ditulis dalam notasi heksadesimal). Sebuah fungsi hash adalah sebuah fungsi matematika, yang mengambil sebuah panjang variabel string input, dan mengkonversikannya ke sebuah string output dengan panjang yang tetap dan biasanya lebih kecil, yang disebut *message-digest atau* nilai-hash [6]. Fungsi hash satu arah adalah fungsi hash yang bekerja satu arah, yaitu suatu fungsi hash yang dengan mudah dapat menghitung nilai-hash dari sebuah pesan, tetapi sangat sukar untuk menghitung pesan dari nilai-hash yang diberikan [7].

Sebuah fungsi hash satu arah, H(M), beroperasi pada suatu pesan M dengan panjang sembarang, dan mengembalikan nilai h yang memiliki panjang tetap. Dalam notasi matematika fungsi hash satu arah dapat ditulis sebagai:

(1) $h = H(M)$
dengan h memiliki panjang b

Ada banyak fungsi yang mampu menerima input dengan panjang sembarang dan menghasilkan output dengan panjang tetap, tetapi fungsi hash satu arah memiliki karakteristik tambahan yang membuatnya satu arah :

Diberikan M, mudah menghitung *h*.
Diberikan h, sulit mengitung M, H(M) = h.
Diberikan M, sulit menemukan pesan lain, M', agar H(M) = H(M').

Dalam dunia nyata, fungsi *hash* satu arah dikembangkan berdasarkan ide sebuah fungsi kompresi. Fungsi satu arah ini menghasilkan nilai-hash berukuran n bila diberikan input berukuran b. Input untuk fungsi kompresi adalah suatu blok pesan dan hasil blok pesan sebelumnya. Sehingga nilai-hash suatu blok M, adalah

(2) $h_i = f(M_i, h_{i-1})$
dengan h_i = nilai-hash saat ini.
M_i = blok pesan saat ini
h_{i-1} = nilai-hash blok pesan sebelumnya.

Fungsi hash sangat berguna untuk menjaga integritas sebuah data. Sudah banyak fungsi hash yang sudah dibuat, namun fungsi hash yang umum digunakan saat ini adalah MD5 dan SHA (Secure Hash Algorithm). Fungsi hash yang baik adalah yang menghasilkan sedikit *collision*.

Contoh penggunaan fungsi hash:

a. Penyimpanan password

MD5 sering juga digunakan untuk menyimpan password dalam database. Daripada menyimpan password dalam bentuk plaintext, lebih baik yang disimpan bukan password, tetapi nilai-hash dari password [15]. Ketika pengguna memasukkan password, nilai-hash password akan dihitung. Nilai-hash dari password yang dimasukkan oleh pengguna ketika login dibandingkan dengan nilai-hash dalam database. Jika cocok, otentikasi berhasil.

Bila pengguna sign-up, maka nilai-hash password akan dihitung dan disimpan dalam database. Misalnya, ketika pengguna mendaftar dengan password "***secure***" maka nilai-hash adalah "1c0b76fce779f78f51be339c49445c49" dan disimpan dalam database. Kemudian login dengan password lainnya, maka nilai-hash tidak akan cocok dengan yang ada dalam database sehingga otentikasi gagal.

b. Verifikasi pesan

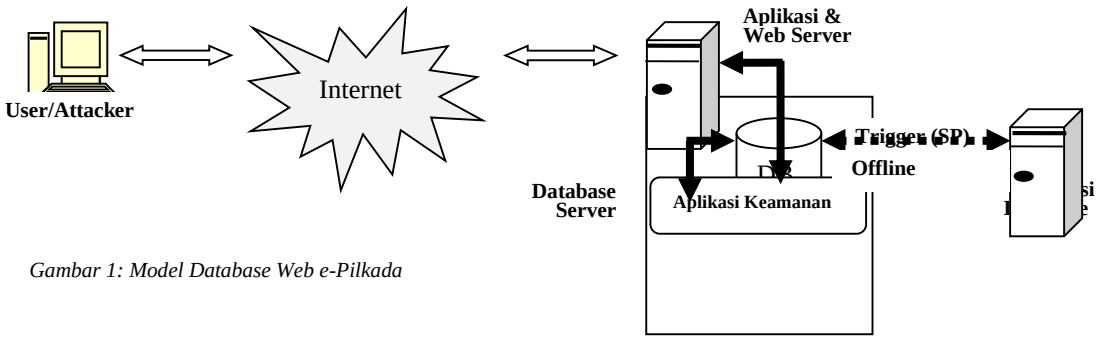
Kadang-kadang kita ingin isi arsip yang disimpan di dalam media penyimpanan komputer atau database tetap terjaga keasliannya. Fungsi hash MD5 juga dapat dipergunakan untuk keperluan tersebut [7]. Caranya, buatkan nilai-hash dari isi arsip dan simpan di dalam database. Verifikasi isi arsip dapat dilakukan secara berkala dengan membandingkan nilai-hash isi arsip sekarang dengan nilai-hash dari arsip asli.

Misalkan pesan pada contoh ini "heard" diubah menjadi "hear", maka pesan:
Sebelum diubah:
"add0135ce7fce6bbf36d240887470789"
Setelah diubah:
"515c93f6d4692a2df8181702b7415c95"
Verifikasi: pesan sebelum dan setelah diubah, tidak sama.
Kesimpulan: informasi atau pesan berubah atau telah mengalami serangan.

MODEL DATABASE E-PILKADA

Pada model database ini, data sensitif terkait hasil pemungutan suara pilkada/pilwali akan disimpan di dalam database dalam bentuk nilai-hash. Model ini menyediakan layanan fungsionalitas keamanan berbasisi fungsi hash dan *recovery* dilakukan terhadap data sensitif sekiranya terjadi perubahan (modifikasi) oleh orang tidak bertanggungjawab, seperti Gambar 1.

Adapun fungsionalitasnya adalah sbb: Pertama adalah rutin untuk login yang dilakukan secara berlapis guna mengontrol user (sistem) dan database (DMBS). Kedua adalah rutin untuk mengontrol integritas data secara periodik (validasi dan verifikasi) pada database dengan aplikasi fungsi hash MD5 berbantuan aplikasi *cron* job atau (php, javascript, dan jquery). Ketiga adalah rutin *data recovery* yang bekerja secara offline.



Gambar 1: Model Database Web e-Pilkada

3. IMPLEMENTASI DAN PENGUJIAN

3.1. Implementasi Prototipe

Ketika user hendak *log-in*, user harus melakukannya secara berlapis (sistem dan aplikasi). Setelah berhasil melalui sistem, data *username* dan *password* aplikasi yang di inputkan akan dihitung nilai *hash*-nya terlebih dahulu, baru kemudian dibandingkan dengan data password di dalam database yang di rekam sebelumnya dalam

bentuk *message-digest*. Jika sama, maka *log-in* pengguna berhasil dan ia dapat mengakses aplikasi sesuai dengan hak akses berdasarkan account utama yang dimiliki.

Gambar 2. Halaman Admin atau Operator

Model menyediakan layanan fungsionalitas keamanan dan *data recovery*. Fungsionalitasi keamanan mengontrol secara periodik database sehingga dapat mengetahui bahwa sebuah data atau informasi telah mengalami perubahan (modifikasi) atau tidak oleh orang tidak bertanggung jawab dengan cara aplikasi melakukan validasi dan verifikasi nilai-hash data perolehan suara arsip. Perubahan data oleh orang tidak bertanggungjawab akan di-*recovery* secara otomatis dengan cara memicu *trigger* secara *offline*.

Gambar 3. Halaman entri dan laporan data pilkada

3.2 Pengujian Model

Skenario:

- Backup dengan replikasi dilakukan dari dbsatu (*online*) ke dbdua (*offline*).
- Database dbsatu dicek secara periodik, setiap 30 detik.
- Apabila ada jumlah perolehan suara pada tblsatu di dalam dbsatu, maka data yang bersesuaian (sesuai id record) pada tbldua dari dbdua akan dibaca dan isi dari tblsatu akan diupdate.
- Apabila proses update berhasil, maka akan dikirim pesan kepada admin bahwa telah terjadi manipulasi dan sukses diperbaiki ke halaman web.

Contoh:

Hasil Pengujian, katakanlah hasil perolehan suara masing-masing cawali disimpan di dalam tblsatu pada database dbsatu dan backupnya pada dbdua, seperti Tabel 1 berikut:

idsatu	cawali	suara	hash1
1	A dan B	4	a87ff679a2f3e71d9181a67b7542122c
2	X dan Y	2	c81e728d9d4c2f636f067f89cc14862c
6	U dan V	10	d3d9446802a44259755d38e6d163e820

iddua	cawali	suara	hash2
1	A dan B	4	a87ff679a2f3e71d9181a67b7542122c
2	X dan Y	2	c81e728d9d4c2f636f067f89cc14862c
3	U dan V	10	d3d9446802a44259755d38e6d163e820

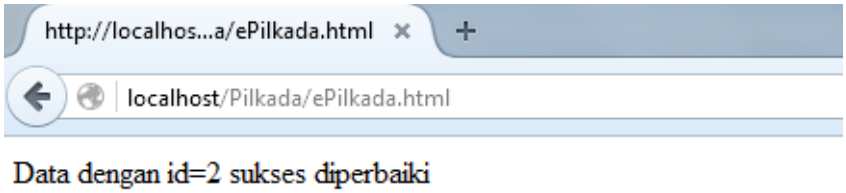
Tabel 1. Perolehan suara pasangan Cawali

- Nilai perolehan suara di dalam tblsatu diubah oleh orang tidak bertanggungjawab yang dalam hal misalnya jumlah suara pada *rekord* 2 (idsatu = 2) dari 2 menjadi 15 secara manual seperti Tabel 2

idsatu	cawali	suara	hash1
1	A dan B	4	a87ff679a2f3e71d9181a67b7542122c
2	X dan Y	15	c81e728d9d4c2f636f067f89cc14862c
6	U dan V	10	d3d9446802a44259755d38e6d163e820

Tabel 2. Perolehan suara pasangan Cawali (yang telah diubah)

- Kemudian database dbsatu diperiksa dan tunggu selama beberapa saat, misalnya 30 detik. Selanjutnya aplikasi akan mengupdate isi tblsatu yang telah berubah dan mengirimkan pesan kepada admin melalui halaman web seperti Gamber 4.



Gamber 4. Pesan kepada Admin

Berikut adalah *script* aplikasi pengujian integritas data sensitif pada database aplikasi e-Pilkada yang diimplementasikan dengan php, javascript, jquery, ajax, dan mysql.

```
//File ePilkada.html
<html>
<head>
<script src="jquery-1.9.1.js"></script>
<script type="text/javascript">
window.setInterval(function(){
  var data;
  $.ajax({
    type: "POST",
    dataType: "json",
    url: "recovery.php",
    data: data,
success: function(data) {
    var n, hasil="";
        for(n in data["idx"])
            hasil += "Data dengan id=" +
           data["idx"][n] + " sukses diperbaiki
           <br />";
        $(".tampil").html(hasil);
    }
  });
  return false;
}, 30000);
</script>
</head>
<body>
<div class="tampil"></div>
</body>
</html>
```

```
//File recovery.php
<?php
function is_ajax() {
  return isset($_SERVER['HTTP_X_REQUESTED_WITH']) &&
strtolower($_SERVER['HTTP_X_REQUESTED_WITH']) ==
'xmlhttprequest';
}

function perbaiki($n, $koneksi){
  mysql_select_db("dbdua", $koneksi);
  $rs = mysql_query("SELECT * from tbldua WHERE iddua=$n",
$koneksi) or die(mysql_error());
  if(mysql_num_rows($rs) > 0){
    $isi = mysql_fetch_assoc($rs);
    mysql_select_db("dbsatu", $koneksi);
    $rs = mysql_query("UPDATE tblsatu SET suara=" .
$isi["suara"] . " WHERE idsatu=" . $n, $koneksi) or
die(mysql_error());
    return $rs;
  }
  else return 0;
}
if (is_ajax()) {
  $koneksi = mysql_pconnect("localhost", "root", "") or
trigger_error(mysql_error(),E_USER_ERROR);
  mysql_select_db("dbsatu", $koneksi);
  $rs = mysql_query("SELECT * from tblsatu", $koneksi) or
die(mysql_error());
  $row = mysql_fetch_assoc($rs);
```

```
do {
   if(MD5($row['suara']) != $row['hash1'])
     if(perbaiki($row['idsatu'], $koneksi))
       $return['idx'][] = $row['idsatu'];
  }while($row = mysql_fetch_assoc($rs));
  echo json_encode($return);
}
?>
```

Gambar 2.

Dari pengujian model atau sistem di atas terlihat bahwa model dapat menjaga integritas dan ketersedian data sensitif yang ada di dalam database seperti diperlihatkan pada Tabel 1. Data perolehan suara oleh pasangan cawali X dan Y telah diubah dari 2 menjadi 15 seperti pada Tabel 2. Tetapi dengan aplikasi pada model ini dapat me*recovery* data tersebut secara otomatis dan menginformasikan ke pengelola sistem yang mengindikasikan bahwa terjadi perubahan dan sudah berhasil diperbaiki Gambar 2.

4. KESIMPULAN DAN SARAN

Model database web e-pilkada berbasis kriptografi fungsi hash dapat mengatasi praktek-praktek serangan oleh pihak tidak bertanggungjawab terhadap situs pilkada. Data sensitif di dalam database dapat di-*recovery* sekiranya terjadi perubahan atau manipulasi oleh pihak tidak bertanggungjawab. Dengan demikian ketersediaan data/informasi dapat terjaga keberadaannya dan masyarakat dapat mengakses kapan saja.

Penelitian lebih lanjut yang dapat dilkukan adalah melengkapi fitur-fitur keamanan dalam aspek lain, seperti bagaimana melindungi data hasil pemungutan suara yang dikirim melalui jaringan Internet. Selanjutnya model ini diimplementasikan dalam bentuk dunia nyata sehingga dapat diterapkan pada pemilu kada.

REFERENSI

[1] Koran Tempo, 2004. Situs KPU dibobol Hacker, Jakarta, 25 April 2004.

[2] Ruzhi, X., Jian G., and Liwu, D. 2010. A Database Security Gateway to the Detection of SQL Attacks, *3rd ICACTE, China*.

[3] Yan, Y., Zhengyuan, S. and Zucheng, D. 2011. The Database Protection System against SQL Attack, *IEEE*, 99-102.

[4] Zhao, Q. and Qin, S. 2008. Studi on Security of Web-based Database, *IEEE Computer Society,Pacific-Aisa Workshop on CIIA*, 902-905.

[5] Yangqing, Z. and Lianming, Z. 2009. Design of A New Web Database Security Model. *IEEE, Electronic Commerce and Security, China*.

[6] Menezes, Oorcshot, and Vanstone, 1996. *Handbook of Applied Cryptography*, CRC Press, Inc. USA.

[7] Munir, R., 2006. *Kriptografi*, Informatika, Bandung.

[8] Date, C.J., 1995. An Introduction to Database System, Addison-Wesley, Reading, MA.

[9] G. S., Khunrana, 1996, Web Database Construction Kit, Waite Group Press, USA.

[10] LPKN UNTAG, 2009. Model e-Pilkada di Propinsi Jawa Timur, Surabaya.

[11] Mahandika, R.J., 2011. Pembuatan Aplikasi Pilkada Kabupaten Magetan Secara Online, Skripsi, AMIKOM, Yogyakarta.

[12] Yusman dan Maryanti, 2012. Rancang Bangun Sistem Informasi Pilkada berbasis Web Kabupaten PIDIE Aceh, Jurnal Litek, Vol. 9 Nomor 2, hal. 133-138.

[13] Aditya W.N. 2011. Perancangan E-Voting Berbasis WEB (Studi Kasus Pemilihan Kepala Daerah Sukoharjo). Skripsi, UIN Sunan Kalijaga Yogyakarta.

[14] Agutina, E,R,, Kurniati A., 2009. Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi pada e-Voting Indonesia, SNI-UVN, Yogyakarta.

[15] Maryanto, B., 2008. Penggunaan Fungsi Hash satu arah untuk Enkripsi Data, Media Informatika, Vol. 7, No. 3, hal. 138-146.