PENGAMANAN SISTEM DAN DATA E-VOTING BERBASIS NETWORK

Muhammad Agreindra Helmiawan
STMIK Sumedang
agreindra@stmik-sumedang.ac.id

Dani Indra Juna
STMIK Sumedang
dani@stmik-sumedang.ac.id

Billy Ramdhani
STMIK Sumedang
billy.ramdhani8@gmail.com

ABSTRACT

Security in a system is vital and can not be ignored at all. System security has an important role to operate a system and keep running in running business processes that support an organization. In every organization, it must have important data and stored in a system mechanism either stand-alone or network-based. Ssytem that has been connected to the network will provide opportunities for the outside world to be able to get information presented by the system in realtime. One example of a system that provides information in realtime is E-Voting, E-Voting system is processing data entered by the user in giving his opinion. If a system that has been corrupted by an outsider or in the sense of an opinion of a user being changed for a particular purpose may be detrimental to the organization. Data security will be very necessary to keep intrupsi on system. The design and application of security methods in the E-Voting system aims to maintain the data provided by the user so that the data is genuine in accordance with the input and the data is original and feasible to be informed

Keywords*: System, Security, Design, E-Voting, Data, Information, Network.*

ABSTRAK

Pengamanan pada sebuah sistem merupakan hal yang vital dan sama sekali tidak dapat diabaikan. Keamanan sistem memiliki peranan penting untuk beroperasinya sebuah sistem dan tetap berjalan dalam menjalankan proses bisnis yang menunjang sebuah organisasi. Dalam setiap organisasi, pasti memiliki data penting dan disimpan dalam sebuah mekanisme sistem baik yang berdiri sendiri ataupun yang telah berbasis network. Sistem yang telah terhubung dengan network akan memberikan peluang bagi dunia luar untuk dapat mendapatkan informasi yang disajikan oleh sistem tersebut secara *realtime*. Salah satu contoh sistem yang memberikan informasi secara *realtime* adalah *E-Voting*, sistem *E-Voting* ini mengolah data yang diinputkan oleh *user* dalam memberikan pendapatnya. Jika sistem yang telah dinterupsi oleh pihak luar atau dalam artian pendapat dari *user* dirubah untuk tujuan tertentu dapat merugikan organisasi. Pengamanan data akan sangat diperlukan untuk menjaga intrupsi terhadap sistem. Rancangan dan penerapan metode keamanan pada sistem *E-Voting* bertujuan untuk menjaga data yang di berikan oleh *user* sehingga data tersebut asli sesuai dengan yang diinputkan dan data tersebut original dan layak untuk diinformasikan.

Kata Kunci: Sistem, Pengamanan, Rancangan, *E-Voting*, Data, Informasi, Network.

1. PENDAHULUAN

1.1 Latar Belakang Masalah

Demokrasi adalah sistem atau bentuk pemerintahan yang mana seluruh rakyat ikut alias terlibat dalam menjalankan roda pemerintahan melalui wakil-wakil rakyat yang telah dipilih oleh rakyat. Sedangkan menurut Abraham Lincoln demokrasi adalah pemerintahan dari rakyat, oleh rakyat, dan untuk rakyat. Salah satu fondasi demokrasi adalah pemungutan suara atau voting. Pemungutan suara (voting) adalah metode yang mana sekelompok orang membuat keputusan, keputusan ini bisa menjadi politik, sosial, atau publik (G.O. Ofori-Dwumfuo dan E. Paatey, 2011).

Voting telah menjadi metode untuk mengambil keputusan penting dalam kehidupan manusia, Pemungutan suara yang kita ketahui dengan metode konvensional, surat suara terbuat dari kertas yang di cetak atau di fotocopy, pada surat suara tersebut terdapat nama, gambar dan nomor urut calon peserta, panitia akan menetapkan cara pemberian suara biasanya dengan mencoblos atau mencontreng surat suara. Telah diketahui saat ini telah berkembang *Voting* dengan media elektronik atau lebih dikenal dengan *E-Voting. E-Voting* mempunyai peranan penting terhadap pemilihan jabatan-jabatan tertentu karena akan sangat membantu dalam menghemat biaya, waktu dan akan sangat berpotensi meningkatkan partisipasi dan jumlah suara.

Sistem *E-Voting* harus direncanakan dengan baik agar nantinya tidak muncul permasalahan-permasalahan baru yang malah akan merugikan pihak-pihak tertentu. Menurut artikel AITP (*Association of Information Technology Professionals*) ada 4 persyaratan agar sistem E-voting dapat dipercaya diantaranya *secure* (aman), *accurate* (akurasi), *re-countable* (dapat dihitung kembali) dan *accessible* (kemudahan untuk mengakses). Syarat *secure* atau segi keamanan adalah salah satu aspek terpenting dalam sebuah sistem informasi, masalah keamanan sering kurang menjadi perhatian dari para perancang dan pengelola sistem informasi, bahkan apabila mengganggu kinerja sistem, masalah keamanan sering ditiadakan.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, dapat dirumuskan masalah penelitian sebagai berikut:

1. Mengamankan data voting yang diberikan oleh *user*
2. Network yang belum aman dari interupsi terhadap sistem.
3. Menerapkan teknik pengamanan pada sistem.

1.3 Ruang Lingkup dan Pembatasan Masalah

Ruang lingkup yang akan dibahas dalam penelitian ini hanya dalam bentuk rancangan untuk pengamanan data voting di dalam sistem yang terhubung ke network.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk merancangan pengamanan pada sistem *E-Voting* yang terhubung ke jaringan komputer. Adapun tujuannya adalah sebagai berikut :

1. Untuk mengamankan data *voting* yang diberikan oleh *user*.
2. Untuk mengantisipasi terjadinya interupsi perubahan data yang disengaja melalui network..
3. Untuk mengetahui dampak pengamanan yang diterapkan pada sistem *E-Voting*.

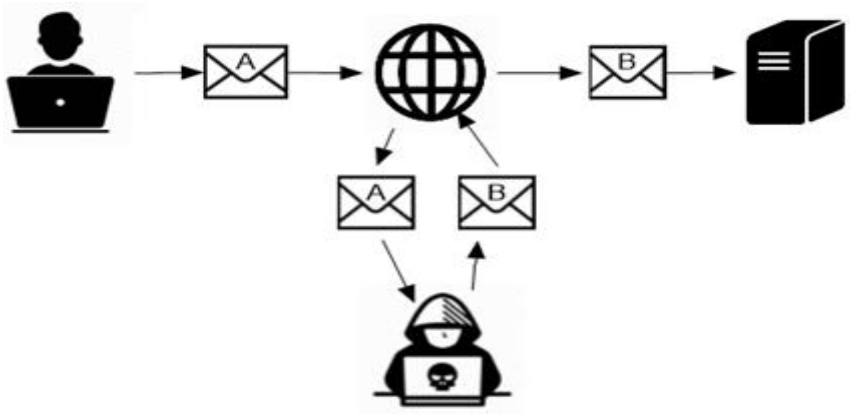
2. METODOLOGI

2.1 Metode Perancangan Sistem

Pada sub ini, penulis menjelaskan proses dan analisis mengenai perancangan keamanan data sistem *e-voting*serta menerapkan algoritma *caesar cipher* pada kode ASCII yang berguna

untuk mengamankan data yang berada pada sistem *e-voting*, yang akan dijelaskan sebagai berikut :

1. Analisis Permasalahan
   Dalam pembahasan sistem keamanan *e-voting* yang sedang penulis bahas yaitu pengamanan data *voting* agar nantinya terjamin kerahasiaannya (*confidentiality*) dan keutuhan data (data integrity).
2. Analisis Data
   Tahapan analisis data merupakan tahapan dimana data apa saja yang akan diamankan dalam sistem *e-voting* dalam hal ini data *voting*/suara dan password setiap para pemilih akan di enkripsi menggunakan algoritma kriptografi.
3. Analisis Keamanan Data *Voting*
   Setiap informasi/data yang terhubung dengan internet akan rentan dengan pencurian atau pengubahan/modifikasi data/informasi itu sendiri oleh orang-orang yang tidak berkepentingan yang akan merugikan beberapa pihak. Dalam kasus yang sedang dibahas oleh penulis, dimana setiap hasil suara *voting* jika tidak di amankan maka ditakutkan akan terjadi perubahan data/suara pada saat pengiriman data/suara. Untuk lebih jelasnya bisa dilihat pada gambar dibawah:



Gambar 1 Proses Merubah Data Suara *Voting*

Deskripsi dari gambar di atas yaitu:

a. Pemilih melakukan *voting*
b. Data suara hasil *voting* dikirim melalui jaringan internet
c. Sebelum masuk ke server cracker akan mencari celah dan masuk kemudian dia merubah surat suara yang tadinya A menjadi B
d. Kemudian *cracker* mengirim data suara yang telah dirubah ke server *e-voting* untuk di simpan.

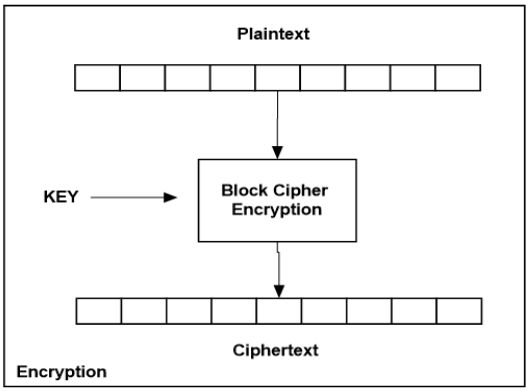
Dalam gambar diatas, cracker sangat mudah untuk merubah data suara *voting* karena suara *voting* dapat dibaca, lebih jelasnya suara *voting* masih berupa *plaintext* atau teks jelas (*cleartext*).Maka dari itu agar data suara tidak dapat dibaca data suara *voting* harus di sandikan. Data suara yang tadinya *plaintext* akan dirubah menjadi *Ciphertext* yaitu teks yang tidak dapat di mengerti dengan menggunkan algoritma kriptografi.

2.2 Proses Penyelesaian Masalah

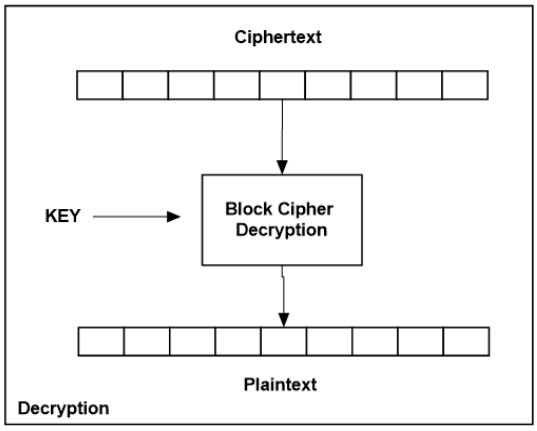
Berdasarkan hasil analisis permasalahan diatas, maka penulis mencoba untuk membuat rancangan untuk mengamankan data suara *voting* dengan menggunakan algoritma kriptografi *Caesar Cipher* dengan Kode ASCII.

1. Analisis *Caesar Cipher*

Pada *Caesar Cipher* cara kerjanya yaitu dengan mensubtitusi *plaintext* dengan kunci yang ada kemudian mengganti huruf *plaintext* dengan huruf pada *ciphertext.*Adapun Rumus Enkripsi *Caesar Cipher* adalah C = E (P) = (P + K) Mod 26 dan Dekripsi adalah P = D (C) = (C – K) mod 26. Lihat gambar 1 – 2 proses Enkripsi dan Dekripsi.



Gambar 2 Plaintext to Ciphertext



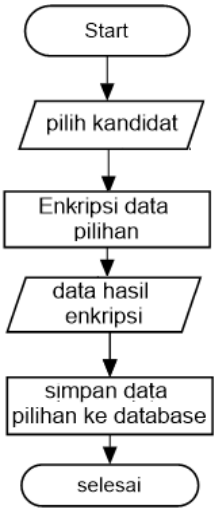
Gambar 3 Ciphertext to Plaintext

2. Analisis Kode ASCII
   Kode ASCII adalah kumpulan kode-kode yang digunakan untuk mempermudah interaksi antara *user* dan komputer. Kode ASCII memiliki komposisi biner sebanyak 8 bit. Mulai dari 00000000 sampai dengan 11111111, total kombinasi yang di hasilkan sebanyak 256 dimulai dari angka 0 sampai dengan 255 dalam bentuk desimal.
3. Penggabungan Algoritma *Caesar Cipher* dengan Kode ASCII
   Untuk memperkuat kerahasian *plaintext* dengan algoritma *Caesar Cipher*. Teknik enkripsi *Caesar Cipher* akan dimodifikasi dengan menggabungkan kode ASCII dengan rumus yang sama tapi dengan jumlah karakter yang berbeda dari 26 menjadi 256 karakter. Dengan menggabungkan Algoritma *Caesar Cipher* dengan kode ASCII akan menghasilkan *plaintext* yang akan sulit diketahui oleh pihak lain karena *plaintext* akan diubah menjadi *ciphertext* dengan rumus C = E (P) = (P + K) Mod 256.

4. Implementasi Algoritma Pada Sistem
   Algoritma *Caesar Cipher* dan kode ASCII akan digunakan untuk mengamankan data *password* dan hasil *voting* setiap pemilih.
   a. Proses Pengamanan Data *Voting*

Pada proses ini setiap data *voting* para pemilih harus di enkripsi untuk mencegah modifikasi data atau perubahan data oleh pihak-pihak yang tidak berkepentingan.Berikut adalah langkah-langkah mengenkripsi data *voting* :

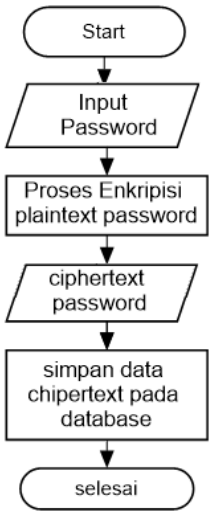
i. Pemilih melakukan *voting*
ii. Pilihannya akan di enkripsi dengan rumus C = E (P) = (P + K) Mod 256 dengan kunci yang telah ditentukan oleh sistem.
iii. Misalkan pilihannya adalah BILLY kemudian akan di enkripsi dengan rumus diatas dengan kunci 10 akan menghasilkan *ciphertext* LSVVc.
iv. Hasil dari enkripsi data akan di simpan ke database dengan format no_induk nama dan hasil pilihan yang telah dienkripsi tadi yaitu LSVVc.



Gambar 4 Proses Enkripisi Data *Voting*

b. Proses Mengamankan *Password*

Setiap data *password* akan di enkripsi untuk mencegah hak pilih digunakan oleh orang lain. Dibawah ini adalah proses enkripsi data *password* :



Gambar 5 Proses Enkripsi *Password*

2.3 Rencana Pengembangan Sistem

Untuk membuktikan apakah algoritma ini dapat mengamankan setiap data pemilihan maka akan dibuatkan sebuah sistem *e-voting* dengan algoritma kriptografi *Caesar Chiper* dengan kode ASCII. Agar sistem yang dibuat dapat berjalan dengan baik maka dibutuhkan spesifikasi lingkungan implementasi sistem dengan *Spesifikasi HardwareProcessor Intel*(R) Core(TM)2 Duo CPU @2.20GHz,Ram 2 Gb, Grafis NVIDIAn GeForce G102M. Spesifikasi

Software diantaranya bahasa pemrograman PHPdengan *Framework CodeIgniter, DataBase MYSQL, Text Editor Sublime Text 3, Sistem Operasi Windows 7 Ultimate 32-bit, Browser Mozila Firefox, Server* dengan *network* LAN dan WAN.

Rencana implementasi diantaranya hasil penelitian yang akan dijabarkan berupa tampilan bagi masing-masing pengguna *e-voting,* termasuk proses pengamanan data menggunakan algoritma yang sedang penulis bahas yaitu *Caesar Chiper* dan Kode ASCII dan akan di interpusi pada sistem *e-voting* tersebut melalui *network.*

3. ANALISA DAN PERANCANGAN SISTEM

Pada tahap ini akan dijelaskan bagaimana proses penghitungan algoritma *Caesar Cipher* dengan kode *ASCII* dalam mengenkripsi dan dekripsi data *voting.*

3.1 Proses Enkripsi

Adapun Proses Enkripsi*Caesar Cipher* yang telah dimodifikasi dengan menggabungkan tabel kode *ASCII* adalah sebagai berikut :

1. Konverikan setiap karakter *plainteks* ke nilai desimal yang ada pada tabel *ASCII.*
2. Sistem akan memberikan kunci enkripsi.
3. Kemudian lakukan proses enkripsi dengan rumus Ci = (Pi+K) Mod 256.
4. Hasil dari proses enkripsi diatas, langkah selanjutnya konversikansetiapnilaiCikekarakter yang adapada table Kode ASCII.

Proses Enkripsi :

Kita menginputkan Plaintext : BILLY

Dengan kunci : 10

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	65	66	67	68	69	70	71	72	73	74

C1 = (P1 + K) Mod 256
= (B + 10)
= (66 + 10)
= 76

C2 = (P2 + K) Mod 256
= (I + 10)
= (73 + 10)
= 83

C3 = (P3 + K) Mod 256
= (L + 10)
= (76 + 10)
= 86

C4 = (P4 + K) Mod 256
= (L + 10)
= (76 + 10)
= 86

C5 = (P5 + K) Mod 256
= (Y + 10)
= (89 + 10)
= 99

Hasil dari Enkripsi Ci : 7683868699 di KonversikankeKarakter yang adapadaTabel ASCII jadiLSVVc.Dan jika di implementasikan ke dalam source code adalah sebagai berikut :

class CaesarCipher

```
{
    public function encrypt($plaintext, $key = 10)
    {
        return $this->run($plaintext, $key);
    }
    protected function run($string, $key)
    {
        return implode('', array_map(function ($char) use ($key) {
            return $this->shift($char, $key);
        }, str_split($string)));
    }
    protected function shift($char, $shift)
    {
        $shift = $shift % 255;
        $ascii = ord($char);
        $shifted = $ascii + $shift;
        if ($ascii >= 0 && $ascii <= 255) {
            return chr($this->wrapUppercase($shifted));
        }
        return chr($ascii);
    }
    protected function wrapUppercase($ascii)
    {
        if ($ascii < 0) {
            $ascii = 256 - (0 - $ascii);
        }
        return $ascii;
    }
}
```

3.2 Proses Dekripsi

Adapun prosesmendekripsi *ciphertext* dari *Caesar Cipher* yang telah di modifikasi dengan tabel *ASCII* adalah :

1. KonversikanSetiapKarakterCikeNilai decimal *ASCII*
2. Deskripsikan setiapnilaidengan rumus Pi = (Ci – K) Mod 256
3. Konversikan nilai Pi ke karakter

L	S	V	V	C
76	83	86	86	99

P1 = (C1 - K) Mod 256
= (76 – 10)
= 66

P2 = (C2 – K) Mod 256
= (83 – 10)
=73

P3 = (C3 – K) Mod 256
= (86 – 10)
= 76

P4 = (C4 – K) Mod 256
= (86 – 10)
= 76

P5 = (C5 – K) Mod 256
= (99 – 10)
= 89

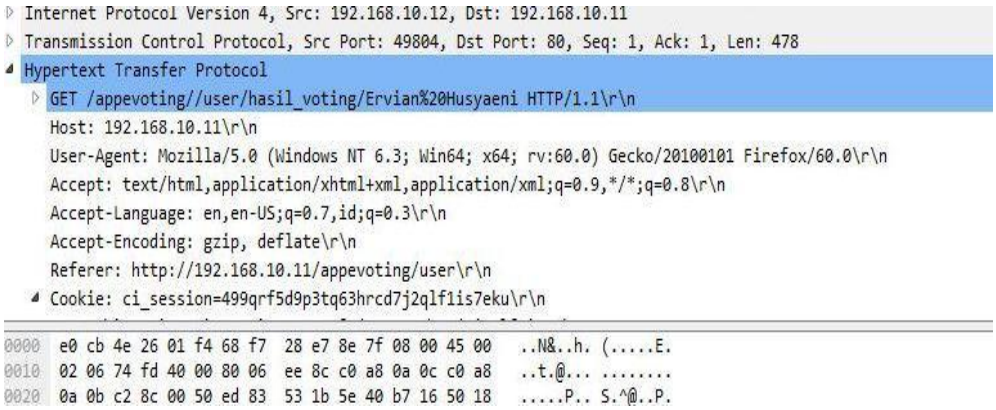
Hasil Dekripsi Pi : 6673767689 di konversikan ke karakter yang ada pada tabel ASCII maka di dapatkan *Plaintext* : BILLY.Pada proses dekripsi ini jika di implementasikan ke sistem dengan *source code* akan menjadi seperti berkut :

```
class CaesarCipher
{
   public function decrypt($ciphertext, $key = -10)
   {
      return $this->run($ciphertext, -$key);
   }
   protected function run($string, $key)
   {
      return implode('', array_map(function ($char) use ($key) {
         return $this->shift($char, $key);
      }, str_split($string)));
   }
   protected function shift($char, $shift)
   {
      $shift = $shift % 255;
      $ascii = ord($char);
      $shifted = $ascii + $shift;
      if ($ascii >= 0 && $ascii <= 255) {
         return chr($this->wrapUppercase($shifted));
      }
      return chr($ascii);
   }
   protected function wrapUppercase($ascii)
   {
      if ($ascii < 0) {
         $ascii = 256 - (0 - $ascii);
      }
      return $ascii;
   }
}
```

3.3 Pengujian Keamanan Sistem

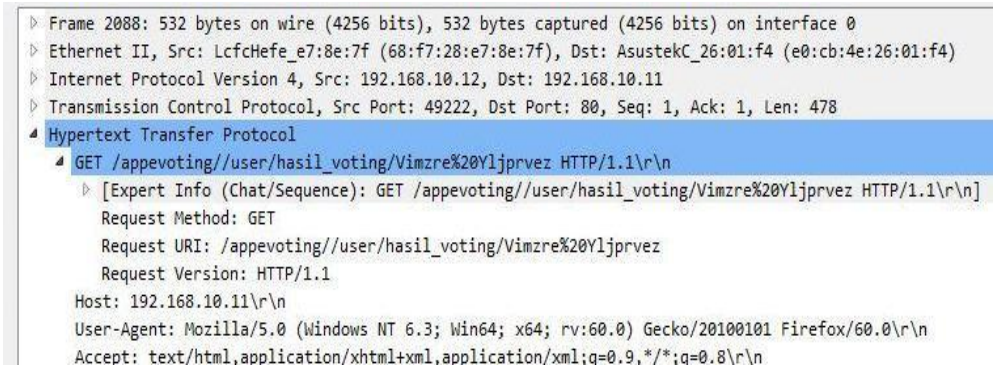
Pengujian dilakukan yaitu menggunakan teknik *sniffing* dengan menggunakan *software wireshark*. Di bawah ini ada 2 gambar hasil *capturing* paket data yang dikirim dari hasil *voting* yaitu hasil *voting* tanpa enkripsi dan hasil *voting* yang telah di enkripsi.

1. Pengiriman paket data hasil vote yang belum dienkripsi



Gambar 6 Pengiriman paket data hasil vote yang belum dienkripsi

2. Pengiriman paket data hasil vote yang telah dienkripsi



Gambar 7 Pengiriman paket data hasil vote yang telah dienkripsi

4. PENUTUP

4.1 Kesimpulan

Kesimpulan dari hasil pengujian yang dilakukan, peneliti menyimpulkan sebagai berikut :

1. Hasil dari penggabungan *Caesar Cipher* dan Kode ASCII dapat menghasilkan karakter huruf yang beragam dan lebih banyak.
2. Dengan menerapkan algoritma *Caesar Cipher* dan kode ASCII pada sistem *e-voting* dapat memenuhi kriteria kemanan *confidentiality* (kerahasiaan), dan *integritydata*(keutuhan data).
3. Sistem *e-voting* dengan menggunakan sistem keamanan kriptografi *Caesar Cipher* dan kode ASCII dapat mengamankan data *voting* dibandingkan dengan sistem *voting* tanpa pengamanan algoritma Kriptografi.

4.2 Saran

Untuk pengembangan selanjutnya peneliti memberikan beberapa saran diantaranya :

1. Mengganti/menambahkan algoritma sistem keamanan dengan menggunakan algoritma yang lebih rumit.
2. Menambahkan fungsi *hash* sehingga tingkat kemanan lebih baik.

DAFTAR PUSTAKA

Adi Purnama, Rahmat. (2015). *Sistem Keamanan E-Voting Menggunkan Kode ASCII.*

Ariyus, Dony. (2008).*Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi.*

G.O. Ofori Dwumfuo and E. Paatey.(2011). *The Design of an Electronic Voting System. Research Journal of information Technology*. 3(2): 91-98.

Haryati, dkk. (2014).*Sistem Pemungutan Suara Menggunakan Model Poll Site E-Voting.*

Helmiawan, (2015). *Internet Positif dengan Metode Web Filtering Layer 7 pada Jaringan Wireless (Study case Hotspot RT 04 Cipeuteuy Baru Sumedang).* Infoman's, 9(2), pp.45-58.

Risnanto, Slamet. (2017). *Aplikasi Pemungutan Suara Electronic/E-voting Menggunakan Teknologi Short Message Service dan AT Command.* Jurnal Teknik Informatika Vol.10 No.1 2017.

Undang-Undang Dasar 1945 : Pasal 28c ayat (1) dan (2).

Wolf, Peter.dkk.(2011).*Policy paper introducing Electronic Voting: Essential Considerations* (Policy Paper, December 2011).