ALGORITMA: Jurnal Ilmu Komputer dan Informatika
Volume: 03, Number: 02, November 2019 ISSN 2598-6341 (online)

Perancangan Sistem Keamanan Aplikasi *E-Voting* Untuk Pemilihan Ketua Badan Eksekutif Mahasiswa Fakultas Teknik UISU Dengan Menggunakan Algoritma MD5

Muhadi M.Ilyas Gultom[1], Darjat Saripurna[2]
Program Studi Teknik Informatika, Fakultas Teknik[1,2]
Universitas Islam Sumatera Utara[1,2]
Ilyasoka8@gmail.com

Abstrak

E-voting Merupakan penggunaan hardware dan software untuk mendirikan sebuah sistem elektronik yang berguna dalam proses pemilihan dengan membuat suara elektronik yang menggantikan kertas suara. E-Voting diperkenalkan oleh beberapa e-goverment terutama di Eropa dalam permintaan untuk melayani ketentuan pemungutan suara dengan menyediakan sistem kontrol, sehingga pemilih dapat memberikan suaranya kapanpun dan dimanapun. Untuk Menghindari segala bentuk kecurangan dan kerusakan pada data yang tentu sangan penting bagi proses voting maka perlu adanya pengamanan data dengan menerapkan kriptografi pada data tersebut. Saat ini ada banyak metode ataupun algoritma yang bias digunakan untuk melindungi data dari berbagai macam serangan, namun tentu masing-masing algoritma memiliki kelebihan dan kekurangannya masing-masing. MD5 adalah algoritma pesan ringkas yang dikembangkan oleh Ron rivest. MD5 sebenarnya telah berakar pada serangkaian algoritma pesan ringkas, yang merupakan pendahulu dari md5, semua dikembangkan oleh Rivest. Message digest asli disebut md.

Kata Kunci : E-voting, Keamanan Data, Algoritma MD5.

Abstract

E-voting Is the use of hardware and software to establish an electronic system that is useful in the electoral process by making electronic votes that replace ballot papers. E-Voting was introduced by several e-Government especially in Europe in a request to serve the voting provisions by providing a control system, so that voters can vote whenever and wherever. To avoid all forms of fraud and damage to data which is certainly very important for the voting process, it is necessary to secure data by applying cryptography to the data. Currently there are many methods or algorithms that can be used to protect data from various types of attacks, but of course each algorithm has advantages and disadvantages of each. MD5 is a concise message algorithm developed by Ron rivest. MD5 has actually been rooted in a series of concise message algorithms, which are the predecessors of md5, all developed by Rivest. The original digest message is called md.

Keywords : E-voting, Data Security, MD5 Algorithm.

I. PENDAHULUAN

Teknologi mengalami kemajuan yang sangat pesat di berbagai bidang, penerapan teknologi pun kian gencar pada hal-hal yang diperlukan untuk mempermudah pekerjaan yang membutuhkan tenaga besar dan sistem yang kompleks. Belum lama ini kita selaku Rakyat Indonesia baru saja melaksanakan pesta demokrasi yaitu pemilu serentak dalam memilih calon presisden dan calon wakil presiden dan juga calon legislatif. Komisi Pemilihan Umum menggunakan Sistem Teknologi Situng(Sistem Hitung) sebagai cara untuk mempermudah masyarakat dalam memantau perkembangan terhadap hasil pemungutan suara. Dalam sekala yang lebih kecil yaitu perguruan tinggi kita mengenal Badan Eksekutif Mahasiswa (BEM) yang ketua dari badan tersebut juga dipilih melalui pemungutan suara oleh seluruh mahasiswa/i.

Pada saat ini proses pemungutan dan perhitungan suara ketua Badan Eksekutif Mahasiswa di Fakultas Teknik Universitas Islam Sumatera Utara masih dilakukan dengan cara konvensional yaitu menggunakan media kertas suara dan perhitungan suara yang masih dengan cara manual. Pemilihan

konvensional dapat menimbulkan berbagai masalah, namun berbagai masalah yang muncul dapat diatasi dengan cara Electronic Voting atau biasa di sebut E-Voting. E-Voting adalah proses pemungutan suara yang menggunakan media teknologi informasi yang bertujuan untuk mempercepat dan mempermudan proses pemungutan dan perhitungan suara pada pemilihan ketua Badan Eksekutif Mahasiswa . Pembuatan sistem E-Voting ini berfokus pada teknologi berbasis web yang menggunakan bahasa pemrograman PHP dan Mysql.

Berdasarkan latar belakang diatas, penulis hendak melakukan penelitian dengan judul "Perancangan Sistem Keamanan Aplikasi E-Voting Untuk Pemilihan Ketua Badan Eksekutif Mahasiswa Fakultas Teknik Uisu Dengan Menggunakan Algoritma Md5".

II. LANDASAN TEORI

A. Pemerintahan Mahasiswa (PEMA)

Pemerintahan mahasiswa merupakan kelengkapan dan nonstruktural pada fakultas yang mempunyai tugas pokok merencanakan dan melaksanakan kegiatan ekstrakulikuler terutama yang bersifat penalaran dan keilmuan sesuai dengan garis-garis besar program yang ditetapkan oleh BAM serta memberikan pendapat, usul dan saran kepada pimpinan Fakultas terutama hal yang berkaitan dengan pelaksanaan fungsi dan pencapaian tujuan pendidikan tinggi. Dalam pelaksanaan tugas pokok dan fungsinya, pengurus PEMA bertanggung jawab kepada mahasiswa pada musyawarah mahasiswa fakultas teknik dan secara administrasi bertanggung jawab kepada pimpinan fakultas yang bersangkutan.

B. *E-Voting*

E-Voting mengacu pada penggunaan Hardware dan software untuk mendirikan sebuah sistem elektronik yang berguna dalam proses pemilihan dengan membuat suara elektronik yang menggantikan kertas suara.

C. Kriptografi

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret(rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika dikirim dari suatu tempat ke tempat lain.

D. Password

Password atau kata sandi dapat digunakan untuk layanan otentikasi, yaitu layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (user authentication atau entity authentication) maupun mengidentifikasi kebenaran sumber pesan.

E. Fungsi Hash

Fungsi hash adalah fungsi yang menerima masukan string yang panjangnya sembarang dan mengkonversinya menjadi string keluaran yang panjangnya tetap (fixed)..

F. Messagae Digest Algoritmh 5 (MD5)

MD5 adalah fungai hash satu arah yang dibuat oleh Ronald Rivest pada tahun 1991. MD5 merupakan perbaikan dari MD4, setelah MD4 berhasil diserang cryptanalyst. Algoritma MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan massage digest yang panjangnya 128 bit.

G. PHP

PHP singkatan dari Hypertext ProProcessor yaitu bahasa pemrograman web server-side yang bersifat opensource. Php merupakan script yang terintegrasi dengan HTML dan berada pada sever (server side HTML embedded scripting).

Berdasarkan defenisi diatas dapat disimpulkan bahwa PHP adalah bahasa pemrograman yang digunakan untuk mengembangkan sebuah Website dinamis yang terintegrasi dengan HTML.

H. HTML

HTML (Hypertext Markup Language) adalah sebuah bahasa yang digunakan untuk membuat sebuah halaman web, menampilkan berbagai informasi ddidalam sebuah penjelajah web internet dan pemformatan hyperteks sederhana yang ditulis dalam berkas format ASCII agar dapat menghasilkan tampilan wujud yang terintegrasi.

I. CSS

CSS merupakan kependekan dari Cascading Style Sheet, berfungsi untuk mempercantik penampilan HTML atau menentukan bagaimana elemen HTML ditampilkan, seperti menentukan posisi, merubah warna teks atau bacground dan lain sebagainya.

J. XAMPP

XAMPP merupakan sebuah tool yang menyediakan beberapa paket perangkat lunak dalam satu buah paket. Dengan menginstal Xampp, anda tidak perlu lagi melakukan instalasi dan mengkonfigurasi web server Apache, PHP, dan MySQL secara manual.

K. MySQL

MySQL adalah sebuah perangkat lunak sistem manajemen basis data data SQL atau yang dikenal dengan DBMS(database management system), database ini multithread, multi-user.

III. METODOLOGI PENELITIAN

A. Proses Pemungutan Suara

Setelah panitia pemilihan membuka pelaksanaan pemungutan suara dan memberikan penjelasan mengenai tata cara pemungutan suara, maka dapat dilaksanakan pemungutan suara sebagai berikut :

1) Para pemilih agar memasuki pintu masuk TPS.
2) Pada saat masuk kedalam TPS.
3) Para pemilih setelah menerima surat suara dari panitia, agar membuka surat suara lebar-lebar.
4) Selanjutnya para pemilih menuju bilik suara untuk menentukan hak pilihnya dengan mempergunakan paku yang telah di sediakan.
5) Setelah melakukan pencoblosan, agar surat suara dilipat kembali sesuai dengan lipatan semula untuk selanjutnya menuju kotak surat suara yang telah disediakan, lalu keluar menuju pintu keluar dan jangan lupa mencelupkan salah satu jari tangan pada tinta yang disediakan.

B. Proses Perhitungan Suara

Pelaksanaan perhitungan suara dimulai paling lama 30 (tiga puluh) menit setelah pelaksanaan pemungutan suara ditutup. Dalam pelaksanaan penghitungan suara panitia harus transparansi.

Penghitungan hasil pemungutan suara dilaksanakan setelah pemungutan suara dinyatakan selesai atau ditutup. Penghitungan hasil pemungutan suara dilakukan oleh Panitia dengan disaksikan oleh masing-masing saksi dari Calon Ketua Badan Eksekutif Mahasiswa Fakultas Teknik. Dalam pelaksanaan penghitungan suara terdapat beberapa jenis surat suara yang dijadikan dasar penghitungan suara diantaranya surat suara sah, surat suara tidak sah dan surat suara blanko, sebagai berikut :

1) Surat suara sah

Surat suara dinyatakan sah apabila :

- Ditandatangani oleh ketua panitia pemilihan serta ada cap atau stempel panitia pemilihan.
- Surat suara dicoblos dengan alat yang disediakan oleh panitia.
- Lubang coblosan masih didalam batasan garis tanda gambar pada satu tanda gambar calon.
- Dalam surat suara terdapat satu lubang coblosan atau lebih tetapi masi berada dalam satu tanda gambar calon.
- Terdapat lebih dari satu berkas coblosan, namun harus ada berkas coblosan pada satu tanda gambar atau di dalam tanda gambar atau garis persegi panjang. Sedangkan berkas coblosan yang

lainnya berada diluar tanda gambar atau garis persegi panjang dan tidak mengenai tanda gambar lainnya.

2) Surat suara tidak sah

Surat suara dinyatakan tidak sah apabila :

- Tidak menggunakan surat suara yang telah ditentukan.
- Tidak terdapat tanda tangan ketua panitia dan cap atau stempel panitia pemilihan.
- Terdapat tanda atau coretan yang menunjukan identitas pemilih.
- Mencoblos lebih dari satu tanda gambar calon.
- Mencoblos tanda gambar selain dari gambar calon yang berhak terpilih.
- Mencoblos diluar tanda gambar yang disediakan.
- Surat suara dicoblos dengan alat lain diluar yang disediakan oleh panitia pemilihan.
- Surat suara yang rusak atau sobek

3) Surat Suara Blanko

Surat suara blanko adalah surat suara yang tidak tercoblos sama sekali.

C. Analisa Permasalahan

Setelah menganalisa proses pemungutan suara dan penghitungan suara yang dilaksanakan secara konvensional. Maka dapat diambil kesimpulan bahwa terdapat beberapa permasalahan atau kekurangan dalam proses sistem pemungutan suara dan penghitungan suara secara konvensional tersebut, sebagai berikut :

1) Data daftar pemilih atau data mahasiswa aktif yang cukup banyak dikumpulkan dengan cara manual dan disimpan hanya menggunakan Ms. Excel. Selain itu pencocokan data antara KTM dan data Mahasiswa aktif kurang efisien digunakan sebagai verifikasi pemungutan suara.

2) Dalam pemungutan suara dengan cara mencoblos memungkinkan terjadi adanya surat suara sobek maupun peserta mencoblos lebih dari satu yang menyebabkan hak suara hilang.

3) Pemungutan suara dengan cara konvensional kurang menjamin keaslian suara pemilih karena memungkinkan terjadi adanya manipulasi pada surat suara.

4) Penghitungan secara manual memiliki kekurangan dari segi ketepatan dan keakuratan penghitungan suara dan memakan waktu yang cukup banyak.

D. Pemecahan Masalah

Dari hasil analisa pemecahan masalah yang ada pada kegiatan pemilihan Ketua Badan Eksekutif Mahasiswa Fakultas Teknik, maka alternatif pemecahan masalah yang diusulkan oleh penulis yang merancang aplikasi e-voting Pemilihan Ketua Badan Eksekutif Mahasiswa Fakultas Teknik pada Universitas Islam Sumatera Utara sebagai berikut :

1) Dengan adanya aplikasi e-voting diharapkan mempermudah penyimpanan data Mahasiswa karena disimpan secara terpusat dalam database, selain itu pencocokan data pemilih lebih mudah.

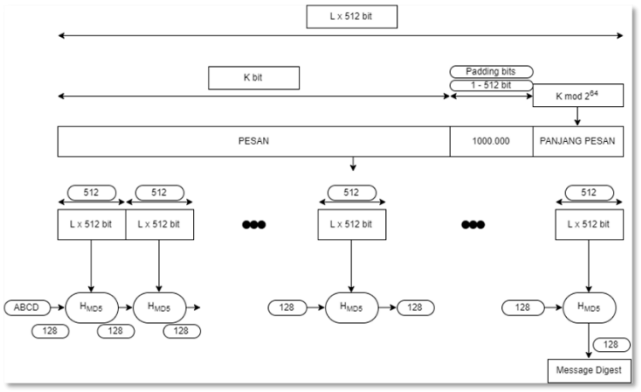
2) Dengan adanya proses authentikasi pada pemungutan suara yang terkomputerisasi sehingga keaslian data pemilih dan suara pemilih diharapkan terjada dengan baik.

3) Diperlukan adanya sistem yang dapat membantu kegiatan pemungutan suara dan penghitungan suara, efektif, efisien untuk mewujudkan pemilihan yang langsung, umum, jujur dan adil.

4) Dengan adanya aplikasi ini diharapkan dapat mengatasi adanya kecurangan atau manipulasi hasil perolehan suara.

5) Mengatasi kejenuhan memilih dengan kertas.

E. Proses Pembuatan Algoritma message Digest 5



Gambar.1. Proses Pembuatan Hasing MD5

Langkah-langkah pembuatan message digest secara garis besar adalah sebagai berikut :

1) Penambahan bit-bit pengganjal (padding bits).

Pesan ditambah dengan sejumlah bit pengganjal sedemikian sehingga panjang pesan (dalam satuan bit) kongruen dengan 448 modulo 512.Bit-bit pengganjal terdiri atas sebuah bit 1 diikuti dengan sisanya bit 0.

2) Penambahan nilai panjaug pesan semula.

Pesan yang telah diberi bit-bit pengganjal selanjutnya ditambahi lagi dengan 64 bit yang menyatakan panjang semula.

3) Inisialisasi penyangga (buffer) MD.

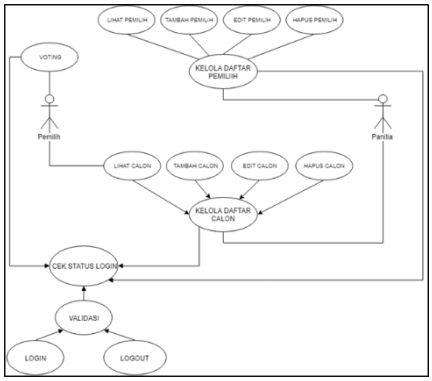
MD5 membutuhkan 4 buah penyangga (buffer) yang masing-masing panjangnya 32 bit. Total panjang penyangga adalah 4 x 32 = 128 bit. Keempat penyangga ini diberi nama A, B, C, dan D. Setiap penyangga diinisialisasi dengan nilai-nilai (dalam notasi HEX) sebagai berikut.

A= 01234567 B=89ABCDEF
C=FEDCBA98
D = 76543210

4) Pengolahan pesan dalam blok berukuran 512 bit.

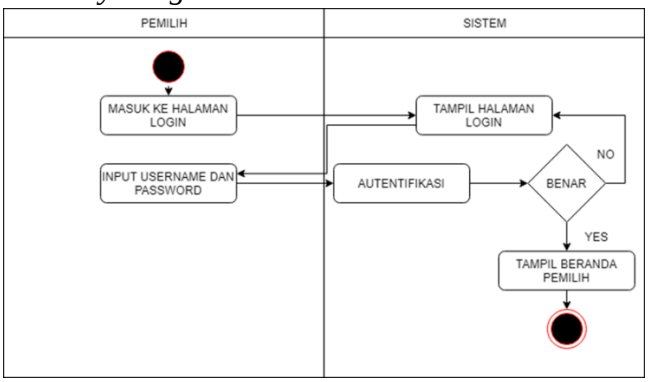
Pesan dibagi menjadi L buah blok yang masing-masing panjangnya 512 bit (YO sampai YL-1). Setiap blok 512-bit diproses bersama dengan penyangga MD menjadi keluaran 128-bit, dan ini disebut proses H.MDs·

F. Diagram Use Case



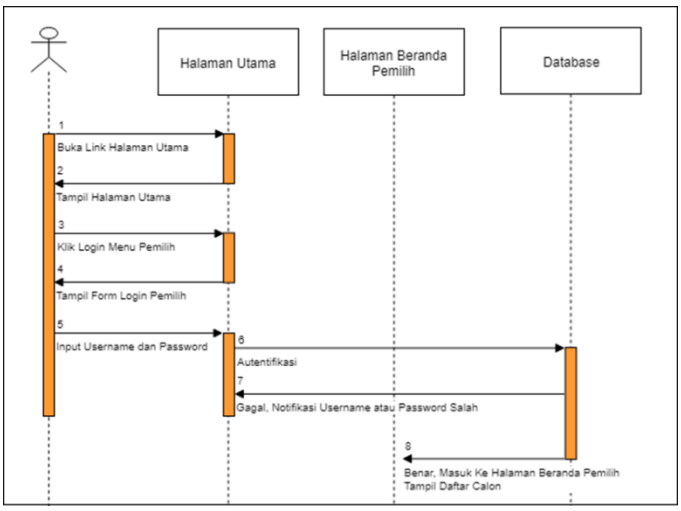
Gambar.2. Usecase Diagram E-Voting

G. Activity Diagram



Gambar.3. Activity Diagram Proses Login Pemilih

H. Sequence Diagram



Gambar.6. Sequence Diagram Login Pemilih

I. Perancangan Tampilan

Gambar.9. Rancangan Tampilan Website

IV. IMPLEMENTASI DAN HASIL

A. Implementasi Algoritma MD5

Tahap imlementasi merupakan dilakukan dengan cara menerapkan algoritma message digest 5 kedalam sistem keamanan data login pada aplikasi e-voting yang dibuat dengan Bahasa pemrograman PHP sedangkan datanya disimpan di database MySQL.

```php
<?php
if(isset($_POST['simpan'])){
    include "../sambungan.php";
    include "../fungsi/upload.php";
    $pemilih=$_POST['username'];
    $sandi   =md5($_POST['password']);
    $nama    =$_POST['nama'];
    $npm     =$_POST['npm'];
    $hp      =$_POST['hp'];
    $email   =$_POST['email'];
    $ik      =$_POST['ik'];
```

Gambar 12. Implementasi Script Pada Login Pemilih

```php
include "sesi.php";
if(isset($_POST['simpan'])){
    include "../sambungan.php";
    include "../fungsi/upload.php";
    $panitia=$_POST['username'];
    $sandi   =md5(trim($_POST['password']));
    $nama    =$_POST['nama'];
    $hp      =$_POST['hp'];
    $email   =$_POST['email'];
    $lokasi  =$_FILES['foto']['tmp_name'];
```

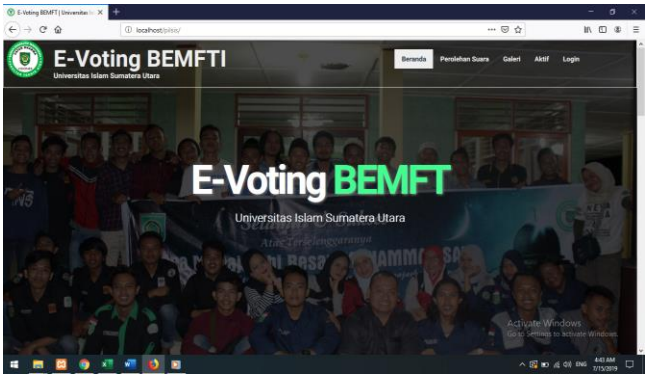
Gambar 12. Implementasi Script Pada Simpan Pemilih

B. Hasil Implementasi Algoritma MD5 pada Database

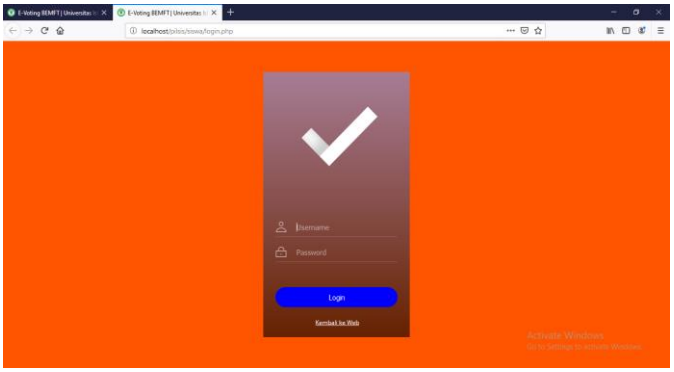
idpanitia	username	password	nama
1	Muhadi	e21721c2088c10b00b7090defd61438e	muhadi m ilyas
2	ilyas	3ea4a8e4d7a95ace878f907ab8b72d1b	ilyas gultom

Gambar.13. Tampilan Password yang telah di Hashing Pada Database

C. Hasil Tampilan



Gambar.14. Hasil Tampilan Website



Gambar.15. Hasil Tampilan Login Pemilih

V.KESIMPULAN DAN SARAN

Berdasarkan pengamatan dari setiap tahap-tahap yang dilakukan oleh maka penulis mengambil kesimpulan sebagai berikut :

1) Aplikasi e-voting semoga dapat membantu kegiatan pemilihan ketua BEM Fakultas Teknik di Universitas Islam Sumatera Utara.
2) Dengan aplikasi e-voting BEMFT diharapkan dapat memperkecil biaya yang.
3) Dengan aplikasi e-voting BEMFT juga diharapkan dapat mempersingkat dalam mengetahui hasil perolehan suara.
4) Perhitungan suara secara elektronik dengan aplikasi e-voting ini menjadi lebih akurat dan hasil perhitungan suara menjadi lebih cepat diperoleh . Berdasarkan kesimpulan diatas maka penulis menyrankan beberapa hal sebagai berikut :

1) Menambahkan pengembangan dengan menambahkan print hasil pemilihan agar data yang lebih akurat dan jelas.
2) Dengan menambahkan tampilan menarik pada halaman utama sebagai simulasi dalam melakukan pemilihan dapat mempermudah pemilih untuk mengetahui hal-hal yang harus dilakukan setelah melakukan login.

DAFTAR PUSTAKA

[1] Anhar. (2010). PHP & MySql Secara Otodidak. Jakarta Selatan: Pt TransMedia.
[2] Ariona, R. (2013). Belajar HTML dan CSS "Tutorial fundamental dalam mempelajari HTML & CSS". ariona.net.
[3] Ariyus, D. (2008). Pengantar Ilmu Kriptografi : Teori Analisis & Implementasi. Yogyakarta: ANDI.
[4] Chen, R. (2011). Intelegent Computing and Information Science. Germany: Pringer-Verlag Berlin Heidelberg.
[5] Hidayat, R. (2010). Cara Praktis Membangun Website Gratis. Jakarta: PT Elex Media Komtindo.
[6] Inayatullah. (2007). Analisis Penerapan Algoritma MD5 Untuk Pengamanan Password. Jurnal Analisis Penerapan Algoritma MD5 Untuk Pengamanan Password.pdf , 1-5.
[7] Kahate, A. (2019). Cryptography and Network Security. India: McGraw Hill Education (India) Private.
[8] Muslihuddin, & Oktafianto. (2016). Analisis dan Perancangan SIstem Informasi Menggunakan Model Terstruktur dan UML. Yogyakarta: ANDI.
[9] Rusmawan, U. (2019). Teknik Penulisan Tugas Akhir dan Skripsi Pemrograman. Jakarta: PT Elex Media Komputindo.
[10] Susrini, N. K. (2010). Website bisnis dengan wordpress. Jakarta: Grasindo.
[11] Sutabri, T. (2012). Analisis Sistem Informasi. Yogyakarta: ANDI.