PENERAPAN AES UNTUK WEBSITE PEMILIHAN KETUA OSIS PADA SMPN 8 PALANGKA RAYA

TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat Penulisan Tugas Akhir pada
Sekolah Tinggi Manajemen Informatika dan Komputer
(STMIK) Palangkaraya



OLEH

EDI SUSANTO
C1555201113
PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
2021

PENERAPAN AES UNTUK WEBSITE PEMILIHAN KETUA OSIS PADA SMPN 8 PALANGKA RAYA

PROPOSAL TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat Penulisan Tugas Akhir pada
Sekolah Tinggi Manajemen Informatika Dan Komputer
(STMIK) Palangkaraya

OLEH

EDI SUSANTO
C1555201113
PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
2021

PERSETUJUAN

PENERAPAN AES UNTUK WEBSITE PEMILIHAN KETUA OSIS PADA SMPN 8 PALANGKA RAYA

Proposal Tugas Akhir Ini Telah Disetujui Untuk Diseminarkan pada
Tanggal 23 Juli 2021

Pembimbing I,	Pembimbing II,
Elia Zakharia, M.T.	Rudini, M.Pd.
NIK. 199205262016104	NIK. 198709172015105

Mengetahui

Ketua STMIK Palangkaraya,

Suparno, M.Kom
NIK. 196901041995105

PENGESAHAN

PENERAPAN AES UNTUK WEBSITE PEMILIHAN KETUA OSIS PADA SMPN 8 PALANGKA RAYA

Proposal Tugas Akhir ini telah Diseminarkan, Dinilai, dan Disahkan
Oleh Tim Seminar pada Tanggal 24 Juli 2021

Tim Seminar Proposal :

1. H. Suratno, S.Kom., M.Si. ….....
   Ketua

2. Elia Zakharia, M.T. ….....
   Sekretaris

3. Rudini, M.Pd. ….....
   Anggota

DAFTAR ISI

PERSETUJUAN ..... **ii**
PENGESAHAN ..... **iii**
DAFTAR ISI ..... **iv**
DAFTAR TABEL ..... **vi**
DAFTAR GAMBAR ..... **vii**
DAFTAR LAMPIRAN ..... **viii**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang Masalah 1
1.2 Perumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan dan Manfaat 4
1.5 Sistematika Penulisan 5
BAB II LANDASAN TEORI **6**
2.1 Tinjauan Pustaka 6
2.2 Kajian Teori 10
2.2.1 Voting 10
2.2.2 Sistem E-Voting 12
2.2.3 Website 14
2.2.4. HTML 15
2.2.5 PHP 16
2.2.6. Database 17
2.2.7. XAMPP 18
2.2.8. Sistem keamanan 18
2.2.9. Organisasi Siswa Intra Sekolah (OSIS) 19
2.3 Algoritma Advance Encryption Standard (AES) 24
2.3.1 Cara kerja AES 256 25
2.3.2 Representasi Data 25
2.3.3 Enkripsi 26
BAB III METODE PENELITIAN **27**
3.1 Lokasi Penelitian 27
3.2 Perencanaan Alat dan bahan 27
3.2.1 Fase Perencanaan Syarat-Syarat 27
3.2.2 Fase Perancangan 29
3.2.3 Fase Konstruksi 31
3.3 Jenis penelitian 31
3.4 Teknik Pengumpulan Data 31
3.5 Analisis Kebutuhan 32
3.6 Desain 33
3.6.1 UML 34
3.6.2 Use Case 34
3.6.3 Activity Diagram 35
3.6.4 Activity Diagram Login 35

3.6.5. Activity Diagram Pemilihan Ketua dan Wakil Osis …….……..36
3.6.6 Class Diagram …….……..……37
3.6.7 Sequence Diagram …….…..……38
3.7 Class Diagram... ……...…….…….39
3.8 User Interface ……..…..……..40
BAB IV IMPLEMENTASI DAN PENGUJIAN 27
4.5 Implementasi ……...……45
BAB V KESIMPULAN DAN SARAN ……50
5.1 Kesimpulan …….50
5.2 Saran ……50
DAFTAR PUSTAKA

DAFTAR TABEL

Tabel 1. Perbandingan penelitian..... **5**
Tabel 2. Skenario pengujian login 49
Tabel 3. Skenario pengujian proses voting.…….,,,49
Tabel 4. Skenario pengujian cetak laporan,……...50

DAFTAR GAMBAR

Gambar 3.0 proses enkripsi dan dekripsi ……..…….....30
Gambar 3.1 Use Case Diagram Perancangan Sistem Pemilihan Ketua Osis.....34
Gambar 3.2 Activity Diagram Login ……35
Gambar 3.3 activity diagram pemilihan ketua dan wakil osis …….36
Gambar 3.4 Class diagram perancangan sistem pemilihan ketua osis.....37
Gambar 3.5 sequence diagram Login ……38
Gambar 3.6 Sequence diagram pemilihan ketua osis ……39
Gambar 3.7 Class diagram… ……40
Gambar 3.8 User Interface Login ……..40
Gambar 3.9 User Interface Halaman Utama ……41
Gambar 4.0 User Interface Data Calon Ketua Osis ……..41
Gambar 4.1 User Interface Data Pengawas ……...42
Gambar 4.2 User Interface Data Pemilih ……..42
Gambar 4.3 User Interface Voting Ketua dan Wakil Osis ……43
Gambar 4.4 User Interface Pengawas ……...43
Gambar 4.5 User Interface Hasil Pemilihan Ketua dan Wakil Osis …….44
Gambar 4.6 Cara Kerja AES ……45
Gambar 4.7 Login ……...…..46
Gambar 4.8 Pemilihan ……...47
Gambar 4.9 Voting ……48

DAFTAR LAMPIRAN

Lampiran 1. Surat tugas pembimbing tugas akhir
Lampiran 2. Lembar wawancara
Lampiran 3. Lembar dokumentasi
Lampiran 4. Kartu kegiatan konsultasi tugas akhir

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Voting adalah kegiatan yang sangat menentukan pada setiap perhelatan pemilihan, banyak varian kepentingan yang harus diakomodir di dalamnya, terutama bagaimana sistem pemilihan itu dilaksanakan, bagaimana regulasi atau peraturan yang disepakati dan menjadi aturan main, siapa yang dipilih dan siapa yang berhak memilih (Zaen dan Putra., 2018). Tidak kalah pentingnya adalah bagaimana proses pemungutan suara dapat menjamin azas langsung, umum, bebas dan rahasia serta bagaimana hasil penghitungan suara dapat berlangsung jujur, transparan, dapat diakses oleh publik (Adhi dan Harjono., 2013). Selama ini, voting dilaksanakan secara centang atau coblos pada kertas suara menjadi pilihan dalam penyelenggaraan pemilu. Metode ini dinilai masih sangat konvensional di tengah kemajuan teknologi dan informasi, memiliki kelemahan dari aspek efisiensi dan efektifitas. Pada proses pemilihan ketua Organisasi Siswa Intra Sekolah (OSIS) kebanyakan juga masih dilakukan secara manual, hal ini dirasa kurang efektif dengan berkembangnya teknologi.

Pembelajaran demokrasi kepada siswa SMP/MA sederajat sangat penting karena siswa adalah pemilih pemula bagi pemilu legislatif dan presiden yang dilaksanakan setiap 5 tahunnya. Kegiatan yang mengadopsi sistem pemilihan yang dilaksanakan oleh KPU ini di dahului oleh penyampaian Visi dan Misi calon ketua OSIS dihadapan seluruh siswa. Prosedur pemilihan ketua OSIS merupakan agenda

tetap bagi pengurus OSIS. Setiap siswa bergantian memberikan hak suaranya di mulai dari siswa kelas VII sampai dengan kelas IX (Yusri Ikhwani., 2018).

Pelaksanaan Pemilihan Ketua OSIS dengan menerapkan sistem pemilihan umum (pemilu) merupakan sebuah proses pembelajaran demokrasi secara langsung bagi seluruh siswa (Amalia Putri Budiarti., 2017). Diharapkan kedepannya para siswa tidak canggung pada saat menghadapi pemilihan umum seperti pemilihan kepala daerah ataupun pemilihan kepala negara, karena sudah memiliki pengalaman pada saat di sekolah. Dan kegiatan ini juga bertujuan untuk menanamkan sikap sportif dan jujur untuk seluruh siswa (Yusri Ikhwani., 2018).

Dengan memanfaatkan teknologi komputerisasi dengan menggunakan aplikasi pemilihan ketua OSIS (e-voting) berbasiskan web bisa membuat kegiatan pemilihan ketua OSIS lebih mudah dalam penyampaian informasi, lebih cepat dalam melakukan perhitungan suara, serta membuat lebih hemat terhadap kertas sehingga hasil yang didapat bisa efektif dan efisien (Risky Yuniarti., 2015).

Hal ini sangatlah penting karena dengan adanya sebuah aplikasi ini maka tidak ada lagi kekurangan informasi, buang-buang kertas dan dapat menghitung hasil perolehan suara dengan cepat dalam pemilihan ketua OSIS dan akan mempermudah siswanya maupun guru yang mengawasi pemilihan ketua OSIS tersebut.

Dengan berkembangnya teknologi e-voting maka sisi keamanan dan kepercayaan publik menjadi hal yang krusial yang perlu diperhatikan dalam penyelenggaraan pemilihan umum (Andri Sulistyo, 2016). Seperti manipulasi data

perolehan suara, sehingga intergritas dalam penyelenggaraan pemilu jauh dari prinsip langsung, umum, bebas dan rahasia.

Untuk itu perlu adanya keamanan dalam menamankan data pemilih dan hasil pemilih seperti penelitian yang dilakukan oleh (Riza, dkk., 2012) mengenai standart keamanan bagi aplikasi dan sistem e-voting nasional dengan menggunakan Teknik kriptografi.

Dalam penelitian ini akan dibuat suatu sistem pemilihan ketua OSIS berbasis web dengan menerapkan alogaritma AES dalam mengamankan sistem. Berbagai cara yang dilakukan untuk menjamin informasi e-voting. Dengan berkembangnya dengan menyembunyikan pesan kriptografi dan bagaimana agar orang lain tidak mengetahui isi pesan atau informasi walaupun pesan tersebut telah ditemukan. Salah satunya adalah dengan menyajikan informasi menjadi suatu kode-kode yang tidak dimengerti, sehingga apabila disadap akan kesulitan untuk mengetahui informasi yang sebenarnya.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah diatas, maka saya ingin mengangkat judul laporan ini tentang **"Penerapan AES Untuk Website Pemilihan Ketua Osis Pada SMPN 8 Palangka Raya"**

1.3 Batasan Masalah

Agar permasalahan dalam analisis ini tidak melebar luar, maka diberikan batasan-batasan untuk pendekatan permasalahan agar lebih terinci dalam pelaksanaannya, yaitu :

a) Sistem yang digunakan berbasis web.

b) Penerapan sistem dilakukan di SMP Negeri 8 Palangka Raya yang berada di jalan tilung.

c) XAMPP digunakan sebagai database server.

d) Code Igniter untuk membantu penyusunan program.

e) Sublime text untuk penyusunan koding.

f) Adobe Photoshop digunakan untuk mengedit banner dan foto calon ketua dan wakil OSIS.

g) Website pemilihan osis ini bersifat offline karena peneliti menghindari dalam pembelian domain.

h) Website pemilihan osis ini ditujukan untuk para guru dan murid di SMP Negeri 8 Palangka Raya.

1.4 Tujuan dan Manfaat

a. Tujuan

Mempermudah para siswa untuk melakukan pemilihan ketua osis di agar sekolah di SMP Negeri 8 Palangka Raya menjadi lebih maju.

b. Manfaat

Adapun manfaat dari proposal tugas akhir ini adalah sebagai berikut :

a) Bagi Penulis

Manfaat yang diperoleh penulis adalah dapat mengimplementasikan ilmu yang telah dipelajari selama kuliah dan meningkatkan kemampuan serta pengetahuan.

b) Bagi Sekolah

Hasil penelitian diharapkan dapat digunakan untuk kemajuan sekolah.

c) Bagi STMIK Palangkaraya

Manfaat yang diberikan kepada kampus STMIK Palangkaraya adalah sebagai penambah literatur pustaka di perpustakaan STMIK Palangkaraya dan juga dapat digunakan sebagai referensi dan dokumen akademik untuk dijadikan acuan bagi Sivitas Akademik STMIK Palangkaraya.

1.5 Sistematika Penulisan

Adapun sistematika penulisan dalam penulisan tugas akhir ini terdiri dari bebrapa bab dan masing-masing bab membahas dan menguraikan pokok permasalahan yang berbeda, sebagai gambaran disini penulis menyertakan garis-garis besarnya yaitu :

BAB I PENDAHULUAN

Bab ini berisikan latar belakang masalah, rumusan masalah, Batasan masalah, tujuan dan manfaat, serta sistematika penulisan

BAB II LANDASAN TEORI

Bab ini berisikan tentang tinjauan pustaka yang diambil dari penelitian yang relevan beserta susunan kajian teori yang disesuaikan dengan tema Tugas Akhir.

BAB III METODE PENELITIAN

Bab ini berisikan tentang tahapan yang dilakukan peneliti dalam mengumpulkan informasi atau data yang dibutuhkan.

BAB II

LANDASAN TEORI

2.1 Tinjauan Pustaka

Dalam suatu penelitian diperlukan dukungan hasil-hasil penelitian yang telah adA sebelumnya yang berkaitan dengan penelitian serupa.Berikut hasil-hasil penelitian yang relevan dan perbandingan penelitian yang telah ada sebelumnya yang serupa dengan penelitian yang sedang dilakukan dan disajikan dalam bentuk tabel.

Tabel 1 Perbandingan Penelitian

No	Nama / Penulis	Topik Penelitian	Metode	Hasil	Perbedaan
1	Irpan Adiputra Pardosi, Ronsen Purba	Pengembangan Web E-Voting Menggunakan Secure Election Protocol (2015)	-	Hasil pengujian yang dilakukan menunjukkan Secure Election Protocol dengan dua panitia sentral telah memenuhi kriteria keamanan yaitu kerahasiaan, integritas,otentikasi, dan anti penyangkalan. Dengan menggunakan algoritma kriptografi AES dalam proses pengiriman data, algoritma RSA untuk mengenkripsi kunci AES dan algoritma SHA-1	Perbedaan Penelitian keamanan menggunakan AES CDC 256 dalam mengamankan data pemilih dan tidak menggunakan secure election protocol

				serta algoritma DSA untuk menandatangani pesan yang dikirim, Kemudian perangkat lunak dapat digunakan sebagai prototipe pemilihan online yang aman dalam sistem yang nyata.	
2	Badrul Anwar, Azanuddin, Nurcahyo Budi Nugroho, Rahmadani Siregar	Aplikasi Pengamanan Dokumen Penjualan Tiket Pesawat Di Pt. Benua Raya Jaya Tour And Travel Menggunakan Metode Advanced Encryption Standard (AES) (2020)	-	Dengan menganalisa permasalahan dan kebutuhan perancangan system pengamanan dokumen penjualan tiket pesawat maka dapat diketahui alur kerja dokumen penjualan tiket pesawat, permasalahan dokumen penjualan tiket pesawat dan kebutuhan yang diperlukan untuk system pengamanan dokumen penjualan tiket pesawat	Perbedaan Penelitian keamanan kami menggunakan AES CDC 256 dalam mengamankan database sedangkan yg ada di jurnal mengamankan dokumen
3	Ryfan Aditya Indra* dan Wahyu Pramusinto	Aplikasi Pengamanan Email Dengan Algoritma Advance Encyption Standard (AES), Rivest Cipher 4 (RC4) Dan Caesar Cipher (2018)		Algoritma Advanced Encryption Standard (AES-128), Rivest Cipher 4 (RC4) dan Caesar Cipher dapat diimplementasikan pada pesan email dalam bahasa pemrograman PHP untuk mengenkripsi dan mendekripsi suatu	Perbedaan Penelitian keamanan kami menggunakan AES CDC 256 dalam mengamankan database sedangkan yg ada di jurnal mengamanka

				isi pesan dan file lampiran.	n email dan lampiran
4	KADRI YUSUF	Penerapan Algoritma MD5 Sebagai Pengaman Akun Pada Aplikasi Web Emusrembang Kota Binjai (2020)	-	Algoritma MD5 dengan fungsi hashnya sangat peka terhadap perubahan pesan, maka algoritma MD5 cocok untuk aplikasi yang menjaga integritas suatu data. Aplikasi algoritma dapat digunakan untuk menjaga keintegritasan data. Dengan aplikasi fungsi hash yang menjadi asas algoritma MD5, perubahan kecil pada data sekalipun dapat terdeteksi. Langkah yang harus ditempuh adalah bangkitkan message digest dari isi arsip menggunakan algoritma MD5. kemudian gabung message digest ke dalam arsip. Verifikasi isi arsip dapat dilakukan secara berkala dengan membandingkan MD	Perbedaan Penelitian keamanan kami menggunakan AES CDC 256 dalam mengamankan database sedangkan yg ada di jurnal menggunakan sistem keamanan md5 dalam enksripsinya

				isi arsip sekarang dan MD dari arsip asli (MD yang telah disimpan sebelumnya). Jika hasilnya berbeda maka telah terjadi perubahan pada arsip	
5	Iman Permana, Mardi Hardjianto, Kiki Ahmad Baihaqi	Securing the Website Login System with the SHA256 Generating Method and Time-based One-time Password (TOTP) (2020)	-	Berdasarkan hasil penelitian yang dilakukan telah menghasilkan sebuah sistem keamanan login web mengimplementasikan One Time Password dengan mengunakan metode pembangkit SHA256 dan Time-based One Time Password (TOTP), dapat ditarik kesimpulan bahwa pengembangan ini mengurangi resiko terjadinya pencuri dikarnakan password yang selalu berubah-ubah setiap 60 detik sekali. Setelah dilakukan pengujian kemanan dari aplikasi yang telah dibuat dilakukan skenario sniffing didapatkan hasil bahwa password dapat di	Perbedaan Penelitian keamanan kami menggunakan AES CDC 256 dalam mengamankan database sedangkan yg ada di jurnal menggunakan sistem keamanan SHA256 dalam enksripsinya

				curi akan tetapi password tidak dapat digunakan kembali untuk melakukan akses masuk kedalam aplikasi webdosen serta pemberian waktu 60 detik dalam setiap perubahan kode dirasa cukup karena setelah dilakukan survei terhadap 20 dosen dari beberapa fakultas menghasilkan rata-rata 29.70 detik.	

2.2 Kajian Teori

2.2.1 Voting

Voting berasal dari kata (vote) dalam Bahasa inggris yang artinya adalah memilih. Dalam ranah politik voting sering kali digunakan bila mana asas musyawarah dan mufakat tidak menghasilkan suatu keputusan yang diinginkan. Sehingga harus diselesaikan dengan melakukan voting.

Dalam perkembangan, teknologi voting mengalami perkembangan yang sangat pesat dan beraneka ragam mulai dari menggunakan kertas sampai memanfaatkan komputer dan jaringan internet. Berikut ini adalah teknologi voting yang umum digunakan yaitu:

1. Surat Suara/Suara Pemilih (Paper Ballots)

Teknologi ini adalah teknologi yang pertama dalam peradaban umat manusia dalam berdemokrasi, dimana kertas suara dijadikan dasar untuk menghitung suara pemilih.

2. Lever Machines

Teknologi berikutnya (Technological Advance adalah Lever Machines yang mulai diperkenalkan pada tahun 1892. Pada teknologi ini tidak terdapat dokumen suara. Pemilih memasukan suara dalam suatu tempat dengan memilih daftar calon dan mengumpulkan masing-masing calon terpilih. Suara dicatat dan dihitung dengan Lever Machines.

3. Punchcards

Teknologi punchcards pertama kali dipakai untuk menghitung suara dengan menggunakan komputer pada tahun 1964. Dalam sistem ini, suara dicatat dengan memilih lubang-lubang pada kartu atau kertas komputer dan selanjutnya komputer akan membaca kartu suara.

4. Marksense Form

Teknologi ini dinamankan optical scan yang digunakan pada tahun 1980. Pada sistem ini pemilih menggunakan bentuk kertas dan menulis pada kotak atau bentuk oval diberi arah panah untuk mengarahkan calon pemilih kemudian dibaca oleh komputer.

5. Electronic Voting

Teknologi electronic voting dimulai pada tahun 1970 yang disebut teknologi pencatatan langsung secara elektronik atau lebih dikenal dengan istilah Direct

Recording Electronic (DRE). Cara memilih dengan sistem ini adalah dengan memilih calon kandidat yang sudah tercetak pada layer komputer.

6. Remote Voting

Remote voting adalah pemungutan suara dari tempat yang berbeda hanya saja cara atau media yang berada atau perangkat yang digunakan bisa berbeda-beda. (Nuryahman 2012).

2.2.2. Sistem E-Voting

Sistem adalah kumpulan dari elemen-elemen yang berinteraksi untuk mencapai suatu tujuan tertentu (Jogiyanto, 2005:2). Sedangkan e-voting adalah proses pemilihan umum yang memungkinkan pemilih untuk mencatatkan pilihannya yang bersifat rahasia secara elektronik yang teramankan (Husni Fahmi dan Dwi Handoko, 2010). Pengertian lain e-voting adalah pemungutan suara yang dilakukan secara elektronik (digital) mulai dari proses pendaftaran pemilih, pelaksanaan pemilihan, penghitungan suara dan pengiriman hasil suara (Ali Rokhman, 2011).

Sistem e-voting ini sudah digunakan dibanyak negara seperti Amerika Serikat, Australia, Austria, Belanda, Belgia, Brazil, Estonia, Inggris, Irlandia, Jerman, Kanada, Norwegia, Perancis, Philipina, Portugal, Spanyol dan Swiss. Sedangkan untuk di Indonesia sendiri sampai tahun 2011 baru satu daerah di Indonesia yang telah menerapkan e-voting dalam proses pemilihan di daerahnya yaitu Kabupaten Jembrana. Hanya saja e-voting yang diterapkan di Jembrana baru sebatas untuk pemilihan Kepala Dusun.

Supaya e-voting dapat diterapkan dengan efektif dan menghasilkan hasil penghitungan suara yang dapat diakui oleh seluruh lapisan masyarakat, di samping prinsip Luber dan Jurdil yang ada pada sistem pemilu sekarang, maka penerapan e-voting harus berdasarkan prinsip-prinsip sebagai berikut :

1. Eligibility

Hanya pemilih yang terdaftar yang dapat melakukan pemilihan.

2. Unreusability

Setiap pemilih hanya bisa memberikan satu kali pilihan.

3. Anonymity

Pilihan pemilih dirahasiakan.

4. Accuracy

Pilihan tidak bisa diubah atau dihapus selama atau setelah pemilihan dan juga tidak bisa ditambahkan setelah pemilihan ditutup.

5. Fairness

Perhitungan suara sebelum pemilihan ditutup tidak bisa dilakukan. (Canard & Sibert 2001).

Dibandingkan dengan berbagai macam proses pemungutan suara yang sudah di uraikan di atas maka e-voting mempunyai beberapa kelebihan diantara lain:

1. Penghitungan dan tabulasi suara lebih cepat.
2. Hasil lebih akurat karena kesalahan manusia dikecualikan.
3. Penanganan yang efisien dari formula sistem pemilu yang rumit yang memerlukan prosedur perhitungan yang melelahkan.

4. Peningkatan tampilan surat suara yang rumit.

5. Meningkatkan kenyamanan bagi para pemilih.

6. Kemungkinan menggunakan layar multibahasa yang dapat melayani para pemilih multibahasa dengan lebih baik dibandingkan surat suara.

7. Pengurangan surat suara yang rusak karena sistem pemilihan dapat memperingatkan para pemilih tentang suara yang tidak sah (walaupun pertimbangannya harus diberikan untuk memastikan bahwa para pemilih bisa tidak memberikan suaranya jika mereka memilih demikian).

8. Berpotensi menghemat biaya dalam jangka panjang melalui penghematan waktu pekerja pemungutan suara dan mengurangi biaya untuk produksi dan distribusi surat suara (Internasional IDEA 2011).

2.2.3 Website

Website adalah sekumpulan halaman web yang saling berhubungan yang umumnya berada pada peladen yang sama berisikan kumpulan informasi yang disediakan secara perorangan, kelompok, atau organisasi.[2] Sebuah situs web biasanya ditempatkan setidaknya pada sebuah server web yang dapat diakses melalui jaringan seperti Internet, ataupun jaringan area lokal (LAN) melalui alamat Internet yang dikenali sebagai URL.

Gabungan atas semua situs yang dapat diakses publik di Internet disebut pula sebagai World Wide Web atau lebih dikenal dengan singkatan WWW. Meskipun setidaknya halaman beranda situs Internet umumnya dapat diakses publik secara bebas, pada praktiknya tidak semua situs memberikan kebebasan bagi publik untuk mengaksesnya, beberapa situs web mewajibkan pengunjung untuk

melakukan pendaftaran sebagai anggota, atau bahkan meminta pembayaran untuk dapat menjadi anggota untuk dapat mengakses isi yang terdapat dalam situs web tersebut, misalnya situs-situs yang menampilkan pornografi, situs-situs berita, layanan surel (e-mail), dan lain-lain. Pembatasan-pembatasan ini umumnya dilakukan karena alasan keamanan, menghormati privasi, atau karena tujuan komersial tertentu.

2.2.4 HTML

HTML kependekan dari HiperText Markup language. Yaitu suatu format data yang digunakan untuk membuat dokumen hypertext yang dapat dibaca dari satu platform komputer ke platform komputer lainnya, tanpa perlu melakukan perubahan apapun. (Winantu & Saputro 2010:1)

HTML pertama kali dikembangkan di CERN yaitu sebuah laboratorium fisika partikel yang berlokasikan di Swiss. Struktur HTML sangat berbeda dengan bahasa pemprograman seperti C++, BASIC, Pascal ataupun Java. Pada HTML tidak bisa digunakan fungsi-fungsi logika seperti IF... ELSE, FOR... NEXT, WHILE...DO dan fungsi-fungsi logika lainnya yang ada pada bahasa pemprograman.

HTML bukan sebuah bahasa pemprograman yang digunakan untuk menulis progam/ aplikasi web. HTML merupakan script untuk membuat sebuah dokumen elektronik yang bisa diterjemahkan oleh banyak sistem yang berbeda (multiplatform) dengan menggunakan software yang disebut browser. HTML terdiri atas tag dan atribut. Keduanya dipakai dalam pengaturan penulisan dokumen

dan bagaimana dokumen itu bisa terlihat lebih menarik dengan adanya tag dan atribut. HTML mempunyai tiga macam tag yaitu :

1. Tag pembuka dimana tag penutup wajib ditulis.

2. Tag pembuka dimana tag penutup bersifat opsional (boleh ditulis, boleh juga tidak ditulis).

3. Tag pembuka yang sama sekali tidak punya tag penutup. (Wahana Komputer 2005:36).

Sebagai catatan, tidak semua tag didukung oleh semua browser. Jika suatu browser tidak mengenali suatu tag tertentu, browser tersebut akan mengabaikan tag yang tidak dikenalinya dan menampilkan isi tag sebagai teks biasa. Aturan penulisan tag :

1. Tag HTML diapit dengan dua karakter kurung bersudut <dan>

2. Tag HTML secara normal selalu berpasangan seperti dan

3. Tag pertama dalam suatu pasangan adalah tag awal dan tag yang kedua adalah tag akhir.

4. Bebas (huruf kapital atau kecil atau campuran huruf besar-kecil) dan tidak case sensitive artinya tag berarti sama dengan <B>.

5. Jika dalam suatu tag ada tag lagi, maka penulisan tag akhir tidak boleh bersilangan, harus berurutan. Misal <l> maka akhirnya harus </l> . (Winantu dan Saputro 2010:4)

2.2.5 PHP

Menurut Siswanto (2012:53) Script PHP berkedudukan sebagai tag dalam bahasa HTML. Sebagaimana HTML (Hyper Text Markup Language) adalah

bahasa standart untuk membuat halaman-halaman web. Model kerja PHP diawali dengan permintaan suatu halaman web oleh browser. Berdasarkan Uniform Resort Locator (URL) atau dikenal dengan sebuah alamat internet, browser mendapatkan alamat dari web server, mengidentifikasi halaman yang dikehendaki dan menyampaikan segala informasi yang dibutuhkan oleh web server. Selanjutnya web server mencarikan berkas yang diminta dan isinya segera dikirim ke mesin PHP dan mesin inilah yang memproses dan memberikan hasil (berupa kode HTML) ke web browser. Selanjutnya web server menyampaikan ke klien.

Banyak sekali kelebihan yang dimiliki PHP dibandingkan dengan bahasa pemrograman yang lain (Suhartono, 2011:2), kelebihan tersebut antara lain kinerja yang tinggi, dapat dihubungkan dengan berbagai macam basis data, pustaka-pustaka built in, biaya rendah, mudah dipelajari, dapat bekerja berbagai macam sistem operasi (portability) dan ketersediaan (availability) kode sumber.

2.2.6. Database

Database adalah tempat penyimpanan file data. Sebagai file data, suatu basis data tidak menyajikan informasi secara langsung kepada penguna. Pengguna harus menjalankan aplikasi untuk mengakses data dari basis data dan menyajikanya dalam bentuk yang bisa dimengerti. Ketika bekerja dengan file-file data, suatu aplikasi harus dikodekan agar bekerja dengan struktur masing-masing file data (Janer Simarmata, 2007).

Database biasanya memiliki dua bagian utama. Bagian pertama adalah file yang memegang basis data fisik. Bagian kedua adalah perangkat lunak sistem manajemen basis data (DBMS) menggunakan aplikasi untuk mengakses data.

Menurut Janer Simarmata (2007:2) DBMS bertanggung jawab menguatkan struktur basis data, diantaranya :

1. Memelihara hubungan antar data di dalam basis data,

2. Memastikan bahwa data tersimpan secara tepat dan menetapkan aturan hubungan data agar tidak dilanggar,

3. Pemulihan (recovery) semu data dari kegagalan sistem. Beberapa software DBMS yang sering digunakan atau yang sudah ada saat ini antara lain MySQL, Postgre SQL, MS SQL, Maria DB, Percona, Mongo DB, Fire Bird, Oracle, Visual Fox Pro, Paradox, DB2, dBase, Microsoft Access dan Ingres.

2.2.7. XAMPP

XAMPP adalah perangkat lunak bebas, yang mendukung banyak sistem operasi, merupakan kompilasi dari beberapa program.

Fungsinya adalah sebagai server yang berdiri sendiri (localhost), yang terdiri atas program Apache HTTP Server, MySQL database, dan penerjemah bahasa yang ditulis dengan bahasa pemrograman PHP dan Perl. Nama XAMPP merupakan singkatan dari X (tempat sistem operasi apapun), Apache, MySQL, PHP dan Perl. Program ini tersedia dalam GNU General Public License dan bebas, merupakan web server yang mudah digunakan yang dapat melayani tampilan halaman web yang dinamis. Untuk mendapatkanya dapat mendownload langsung dari web resminya.

2.2.8. Sistem keamanan

Keamanan komputer adalah suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada komputer. Sasaran keamanan

komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian atau korupsi, atau pemeliharaan ketersediaan, seperti dijabarkan dalam kebijakan keamanan.

Sistem keamanan komputer merupakan sebuah upaya yang dilakukan untuk mengamankan kinerja dan proses komputer. Penerapan computer security dalam kehidupan sehari-hari berguna sebagai penjaga sumber daya sistem agar tidak digunakan, modifikasi, interupsi, dan diganggu oleh orang yang tidak berwenang. Keamanan bisa diindentifikasikan dalam masalah teknis, manajerial, legalitas, dan politis. computer security akan membahas 2 hal penting yaitu Ancaman (threats) dan Kelemahan sistem (vulnerabillity).

2.2.9. Organisasi Siswa Intra Sekolah (OSIS)

OSIS adalah satu-satunya organisasi kesiswaan di sekolah dan kursus untuk mencapai tujuan pembinaan kesiswaan serta pengembangannya dan tidak ada hubungannya dengan organisasi OSIS di sekolah lain.

a. Pengertian OSIS

Organisasi Siswa Intra Sekolah (OSIS) adalah suatu organisasi yang berada di tingkat sekolah di Indonesia yang dimulai dari Sekolah Menengah Pertama (SMP) dan Sekolah Menengah Atas (SMA). OSIS diurus dan dikelola oleh murid-murid yang terpilih untuk menjadi pengurus OSIS. Biasanya organisasi ini memiliki seorang pembimbing dari guru yang dipilih oleh pihak sekolah. Anggota OSIS adalah seluruh siswa yang berada pada satu sekolah tempat OSIS itu berada.

Dalam upaya mengenal, memahami dan mengelola OSIS perlu kejelasan mengenai Pengertian, Tujuan, Fungsi, dan Struktur OSIS. Dengan mengetahui

pengertian, tujuan,fungsi, dan struktur yang jelas, maka akan membantu Pembina pengurus dan perwakilan kelas untuk mendayagunakan OSIS ini sesuai dengan fungsi dan tujuannya. Pengertian OSIS , meliputi :

1. Secara Sistematis

Di dalam Surat Keputusan Direktur Jendral Pendidikan Dasar dan Menengah Nomor 226/C/Kep/0/1992 disebutkan bahwa organisasi kesiswaan di sekolah adalah OSIS. OSIS adalah Organisasi Intra Sekolah yang masing-masing kata mempunyai pengertian, sebagai berikut :

a) Organisasi: merupakan kelompok kerja sama antara pribadi yang diadakan untuk mencapai tujuan bersama. Organisasi dalam hal ini dimaksudkan sebagai satuan atau kelompok kerjasama para siswa yang dibentuk dalam usaha mencapai tujuan bersama, yaitu terwujudnya pembinaan siswa.

b) Siswa: peserta didik pada satuan pendidikan dasar dan menengah.

c) Intra: berarti terletak di dalam dan di antara sehingga suatu organisasi siswa yang ada dalam dan di lingkungan sekolah.

d) Sekolah: satuan pendidikan tempat menyelenggarakan kegiatan belajar mengajar, yang dalam hal ini Sekolah Dasar dan Sekolah Menengah yang sederajat.

2. Secara Organisasi

OSIS adalah satu-satunya wadah organisasi siswa yang sah di sekolah. Oleh karena itu, setiap sekolah wajib membentuk Organisasi Siswa Intra Sekolah (OSIS) yang tidak mempunyai hubungan organisatoris dengan OSIS di sekolah lain dan tidak menjadi bagian dari organisasi lain yang ada di luar sekolah

3. Secara Fungsional

Dalam rangka pelaksanaan kebijakan pendidikan, khususnya di bidang pembinaan kesiswaan, arti yang terkandung lebih jauh dalam pengertian OSIS adalah sebagai salah satu dari empat jalur pembinaan kesiswaan, di samping ketiga jalur yang lain yaitu latihan

kepemimpinan, ekstrakurikuler, dan wawasan wiyatamandala.

4. Secara Sistematik

Apabila OSIS dipandang sebagai suatu sistem, berarti OSIS sebagai tempat kehidupan berkelompok siswa yang bekerja sama untuk mencapai tujuan bersama. Dalam hal ini OSIS dipandang sebagai suatu sistem, dimana sekumpulan para siswa mengadakan koordinasi dalam upaya menciptakan organisasi yang mampu mencapai tujuan. Oleh karena itu, OSIS dipandang sebagai suatu sistem ditandai beberapa ciri pokok, yaitu:

a) Berorientasi pada tujuan

b) Memiliki susunan kehidupan berkelompok

c) Memiliki sejumlah peranan

d) Terkoordinasi

e) Berkelanjutan dalam waktu tertentu

b. Tata cara pemilihan Perwakilan Kelas dan pemilihan Pengurus OSIS

adalah sebagai berikut:

1. Pemilihan Pengurus Harian Majelis Permusyawaratan Kelas (MPK)

a) Pemilihan ini digunakan untuk memilih Ketua MPK, Wakil Ketua MPK, beserta Sekretaris dan Bendahara MPK.

b) Calon Pengurus Harian wajib mengikuti seleksi yang diadakan oleh MPK/OSIS.

c) Sedikitnya hasil seleksi menghasilkan 4 Calon Ketua MPK, 3 Calon Sekretaris MPK< dan 3 Calon Bendahara MPK.

d) Kandidat yang berhasil terpilih akan mengikuti mekanisme yang telah ditetapkan sesuai Sidang Pleno MPK sebelumnya.

e) Pemilihan dapat dilakukan dengan metode Pemungutan Suara dan/atau Musyawarah Mufakat.

f) Syarat Melakukan Pemilihan melalui metode Pemungutan Suara:

1) Sedikitnya setiap kelas mengirimkan 1 orang perwakilan kelasnya, dan Maksimal mengirimkan 3 orang untuk mengikuti Pemungutan Suara.

2) Kandidat Pengurus Harian MPK wajib mengikuti jalannya Pemungutan Suara.

3) Pemungutan Suara dikatakan Syah apabila dihadiri oleh Pembina MPK/OSIS.

4) Penghitungan dilakukan secara terbuka dan terang-terangan dihadapan peserta Pemungutan Suara.

g) Syarat Melakukan Pemilihan melalui metode Musyawarah Mufakat:

1) Sedikitnya Anggota Perwakilan Kelas yang hadir 2/3 dari total Anggota Perwakilan Kelas seluruhnya.

2) Pimpinan Musyawarah ialah Ketua MPK yang sedang menjabat.

3) Kandidat Pengurus Harian MPK dilarang keras mengikuti jalannya Musyawarah.

4) Musyawarah Mufakat dikatakan Syah apabila dihadiri oleh Wakil Kepala Sekolah bidang Kesiswaan.

5) Musyawarah dikatakan selesai apabila terjadi Mufakat dan tidak terdapat pertentangan pendapat lagi.

2. Pemilihan Perwakilan Kelas

a) Pemilihan perwakilan kelas diselenggarakan pada awal tahun pelajaran baru, hari pertama masuk sekolah, semua siswa yang duduk di kelas yang bersangkutan memilih ketua dan wakil ketua kelas

b) Anggota perwakilan kelas terdiri dari 2 (dua) orang siswa tiap kelas yang dipilih secara langsung oleh anggota kelasnya yang dihadiri oleh wali kelas

c) Anggota perwakilan kelas dapat dirangkap oleh ketua dan wakil ketua kelas

d) Kepala Sekolah selaku Ketua Pembina atau menunjuk wakil kepala sekolah segera mengundang semua anggota perwakilan kelas untuk membentuk dan mengesahkan pengurus kelas.

3. Pemilihan atau pembentukan Pengurus OSIS

a) Pemilihan/pembentukan pengurus OSIS diselenggarakan selambat lambatnya 1 (bulan) setelah terbentuknya perwakilan kelas.

b) Penyelenggara Pemilihan atau Pembentukan pengurus OSIS dibentuk oleh Kepala Sekolah, dengan unsure-unsur panitia pemilihan OSIS terdiri dari: pembina OSIS, pengurus OSIS lama, perwakilan Kelas, siswa.

c) Ketua dan wakil ketua OSIS dipilih secara langsung dalam satu paket oleh seluruh siswa dalam waktu 1 (satu) hari dan hasilnya diumumkan secara langsung.

d) Ketua dan wakil ketua terpilih segera melengkapi kepengurusan OSIS selambat-lambatnya 1 (minggu) setelah pemilihan.

2.3 Algoritma Advance Encryption Standard (AES)

AES termasuk jenis algoritma kriptografi yang sifatnya simetri dan cipher blok. Algoritma ini menggunakan kunci yang sama saat enkripsi serta masukkan dan keluaran berupa blok dengan jumlah bit tertentu.

Input dan ouput dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi ciphertext. Algoritma AES merupakan algoritma simetris yaitu menggunakan kunci yang sama untuk proses enkripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe : AES-128, AES-192 dan AES-256. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu round key untuk setiap proses putaran. Proses putaran enkripsi AES-128 dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut :

1. Addroundkey
2. Putaran sebanyak a-1 kali, proses yang dilakukan pada setiap putaran adalah: SubBytes, ShiftRows, MixColumns, dan AddRoundKey.
3. Final round adalah proses untuk putaran terakhir yang meliputi SubBytes, ShiftRows, dan AddRoundKey. Proses putaran juga dikerjakan sebanyak 10 kali (a=10), yaitu sebagai 1.

Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Ilustrasi proses enkripsi AES dapat digambarkan seperti pada gambar di bawah ini :

2.3.1 Cara kerja AES 256

AES memiliki blok masukan dan keluaran kunci 256 bit untuk tingkat keamanan tinggi. Setiap masukan 128 bit plaintext dimasukkan ke dalam state yang berbentuk bujur sangkat berukuran 4x4 byte. State ini di XOR dengan key, kemudian diolah sebanyak 10 kali dengan subtitusi transformasi linear addkey. Maka diperoleh sebuah ciphertext. Dan cara operasi pada AES adalah sebagi berikut:

1. Ekspansi kunci utama (256 bit menjadi 1408 bit)
2. Pencampuran subkey
3. Ulang dari i=1 sampai i=14 transformasi : SubByte, ShiftRow, MixColumn
4. Pencampuran subkey (XOR)
5. Transformasi : SubByte dan ShiftRow
6. Pencampuran Subkey

Dan dari beberapa operasi maka akan di terapkan cara kerja dari aes adalah sebagai berikut :

2.3.2 Representasi Data

Input dan output dari algoritma AES terdiri dari urutan data sebesar 256 bit. Urutan data yang sudah terbentuk dalam satu kelompok 256 bit tersebut disebut juga 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. Urutan bit diberi nomor urut dari 0 sampai dengan n-1 dimana n adalah nomor urutan. Urutan data 8 bit secara berurutan disebut sebagai byte dimana byte ini adalah unit dasar dari operasi yang akan dilakukan pada blok data.

2.3.3 Enkripsi

Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dikopikan ke dalam state akan mengalami transformasi byte AddRoundKey. Setelah itu, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai round function. Round yang terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns.

BAB III

METODE PENELITIAN

3.1 Lokasi Penelitian

Lokasi penelitian di smp 8 palangka raya dalam upaya menerapkan pemilihan ketua osis secara E-Voting agar memudahkan dalam pemilihan ketua osis

3.2 Perencanaan Alat dan bahan

Penelitian dilakukan dengan menggunakan metode pengembangan sistem model pendekatan RAD (Rapid Application Development). Penulis menggunakan model RAD karena melihat dari aplikasi yang dikembangkan adalah aplikasi yang sederhana dan tidak membutuhkan waktu yang lama, metode RAD adalah metode yang diperuntukkan untuk jangka pendek sesuai dengan aplikasi yang dikembangkan. Berikut adalah penjelasan masing-masing fase RAD dalam penelitian ini.

3.2.1 Fase Perencanaan Syarat-Syarat

1. Analisis Kebutuhan Masalah

Permohonan perencanaan kebutuhan penelitian yang dilakukan, maka peneliti dapat menganalisis bahwa pemilihan masih dilakukan dengan cara tradisional ini telah menyebabkan lamanya pemilihan yang dilakukan. Oleh karena itu, diperlukan sebuah aplikasi pemilihan ketua osis yang memiliki sistem keamanan AES data yang mudah digunakan dan dapat menjamin kerahasiaan data mereka.

2. Tujuan

Berdasarkan pada analisis kebutuhan di atas, maka tujuan penelitian ini adalah untuk membuat suatu aplikasi pemilihan ketua osis smp 8 palangka raya serta menerapkan enkripsi yang mengimplementasikan metode Advance Encryption Standard sehingga dapat menjaga kerahasiaan data.

3. Syarat-syarat

Untuk mewujudkan tujuan tersebut dibutuhkan beberapa syarat minimum dalam pembuatan aplikasi keamanan data ini yaitu meliputi hal-hal sebagai berikut :

a. Web server

Web server merupakan syarat mutlak suatu aplikasi berbasis web. Web server merupakan platform untuk menjalankan suatu aplikasi berbasis web. Untuk pengembangan aplikasi ini dibutuhkan minimum Web Server Apache 2.4.48

b. Bahasa Pemrograman

Bahasa pemrograman dibutuhkan untuk dapat membangun sebuah aplikasi, agar komputer dapat melakukan berbagai operasi dan fungsi sesuai dengan keinginan user. Untuk itu dibutuhkan suatu bahasa pemrograman yang dapat digunakan untuk membuat aplikasi client server. Bahasa pemrograman minimum yang dibutuhkan dalam pengembangan aplikasi ini adalah PHP 8.0.7.

c. Database

Perancangan tabel-tabel akan digunakan untuk pelengkap program seperti proses login serta proses penamaan dan penyimpanan file enkripsi. Database yang dibutuhkan adalah database MySQL 5.1.1

Spesifikasi perangkat lunak dan perangkat keras minimum yang diperlukan dalam pembuatan aplikasi ini adalah sebagai berikut :

a. Perangkat Lunak :

1. Paket web server

(Apache 2.4.48, PHP 8.0.7, MySQL 5.1.1)

2. Adobe Photoshop.

3. Sublime

4. Google Chrome

5. Microsoft Windows 10.

b. Perangkat Keras :

1. Processor Intel Core I5 Gen 8.

2. Harddisk 1 TB.

3. Memory SDR 2 GB.

4. Monitor dengan resolusi 1366 x 768 pixel.

3.2.2 Fase Perancangan

Pada tahap ini dilakukan perancangan proses yaitu perancangan proses-proses yang akan terjadi di dalam sistem.

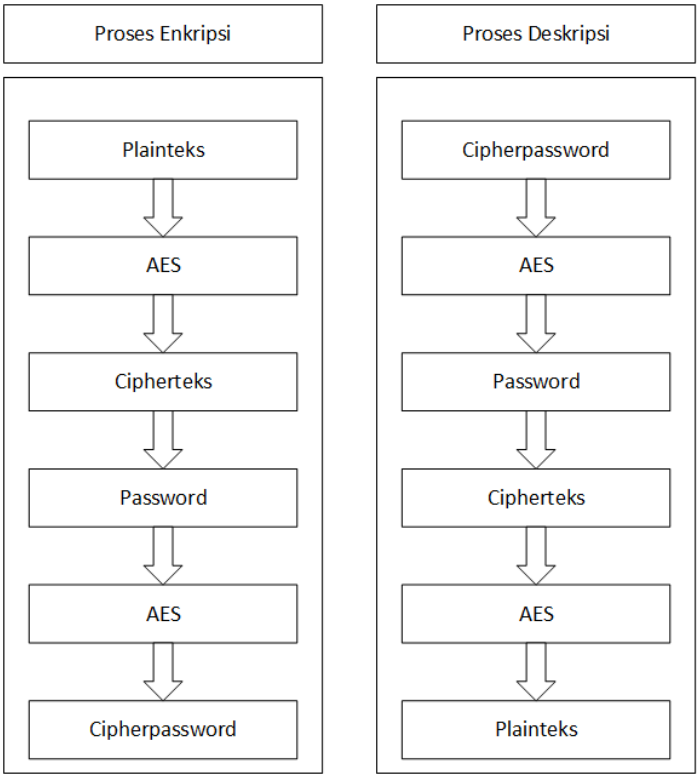
1. Perancangan Proses

Aplikasi ini menggabungkan dua metode enkripsi. Pada proses enkripsi, data dienkripsi menggunakan metode enkripsi Advance Encryption Standard. Setelah selesai, kunci yang digunakan untuk enkripsi dengan Advance Encryption Standard tadi dienkripsi dengan menggunakan metode enkripsi Advance Encryption Standard, dan string hasil enkripsi password tersebut disimpan di basis data.

Pada proses dekripsi, data terenkripsi yang dihasilkan pada proses enkripsi akan diubah menjadi data semula dengan cara membalik proses enkripsi. Pada proses ini

pertama- tama, password didekripsi menggunakan kunci metode dekripsi Advance Encryption Standard. Setelah selesai maka data terenkripsi didekripsi dengan kunci tadi menggunakan metode dekripsi Advance Encryption Standard. Setelah proses dekripsi selesai data terenkripsi akan kembali ke tipe semula.

Agar memperjelas gambaran proses enkripsi dan dekripsi, dapat dilihat pada gambar 3.0.



Gambar 3.0 proses enkripsi dan dekripsi

2. Perancangan Basis Data

Pada aplikasi ini digunakan database sebagai pelengkap program seperti proses login dan proses penyimpanan data enkripsi. Database yang digunakan adalah database MySQL.

3. Perancangan Antarmuka Pemakai (User Interface)

Perancangan antarmuka pemakai memberikan fasilitas komunikasi antar pemakai dan sistem, memberikan berbagai fasilitas informasi dan berbagai keterangan yang bertujuan untuk membantu mengarahkan alur penelusuran masalah sampai ditemukan solusi.

3.2.3 Fase Konstruksi

Pada tahap ini dilakukan pembuatan program terhadap rancangan-rancangan yang telah didefinisikan. Pembuatan program yang dilakukan menggunakan bahasa pemrograman PHP yang dibuat dengan menggunakan Sublime.

3.3 Jenis penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode penelitian yang digunakan adalah metode penelitian Deskriptif. Metode analisis deskriptif kualitatif yaitu suatu metode penelitian yang dilakukan untuk menggambarkan proses atau peristiwa yang sedang berlaku pada saat ini di lapangan yang di jadikan objek penelitian, kemudian data atau informasinya di analisis sehingga di peroleh suatu pemecahan masalah.

3.4 Teknik Pengumpulan Data

Teknik pengumpulan data dalam kegiatan pembuatan website ini dilakukan dengan 3 cara, yaitu: studi pustaka, wawancara, dan observasi.

1. Studi pustaka, yaitu pengumpulan data dari perpustakaan yang dilakukan dengan cara membaca dan mempelajari buku literatur, majalah, artikel internet dan informasi lainnya sebagai bahan tinjauan pustaka yang berkaitan dengan pembuatan website ini.

2. Wawancara, mencari data dengan cara melakukan tanya jawab pada pihak terkait, yang mempunyai wewenang atas data-data yang berhubungan dengan obyek penelitian (Pemilihan Ketua Osis SMP 8 Palangka Raya).

3. Observasi, pada tahapan ini diadakan kegiatan pengamatan mengenai struktur dan navigasi website yang akan dibangun, agar dapat menjadi website yang sempurna.

3.5 Analisis Kebutuhan

Permohonan perencanaan kebutuhan yang dilakukan, maka peneliti dapat menganalisis bahwa pemilihan masih dilakukan dengan cara tradisional ini telah menyebabkan lamanya pemilihan yang dilakukan. Oleh karena itu, diperlukan sebuah aplikasi pemilihan ketua osis yang memiliki sistem keamanan AES data yang mudah digunakan dan dapat menjamin kerahasiaan data mereka.

a. Web server

Web server merupakan syarat mutlak suatu aplikasi berbasis web. Web server merupakan platform untuk menjalankan suatu aplikasi berbasis web. Untuk pengembangan aplikasi ini dibutuhkan minimum Web Server Apache 2.4.48

syarat dalam pembuatan aplikasi keamanan data ini yaitu meliputi hal-hal sebagai berikut :

b. Bahasa Pemrograman

Bahasa pemrograman dibutuhkan untuk dapat membangun sebuah aplikasi, agar komputer dapat melakukan berbagai operasi dan fungsi sesuai dengan keinginan user. Untuk itu dibutuhkan suatu bahasa pemrograman yang dapat digunakan untuk

membuat aplikasi client server. Bahasa pemrograman minimum yang dibutuhkan dalam pengembangan aplikasi ini adalah PHP 8.0.7.

c. Database

Perancangan tabel-tabel akan digunakan untuk pelengkap program seperti proses login serta proses penamaan dan penyimpanan file enkripsi. Database yang dibutuhkan adalah database MySQL 5.1.1

Spesifikasi perangkat lunak dan perangkat keras yang digunakan dalam pembuatan aplikasi ini adalah sebagai berikut :

a. Perangkat Lunak :

1. Paket web server

(Apache 2.4.48, PHP 8.0.7, MySQL 5.1.1)

2. Adobe Photoshop.
3. Sublime
4. Google Chrome
5. Microsoft Windows 10.

b. Perangkat Keras :

1. Processor Intel Core I5 Gen 8.
2. Harddisk 1 TB.
3. Memory SDR 2 GB.
4. Monitor dengan resolusi 1366 x 768 pixel.

3.6 Desain

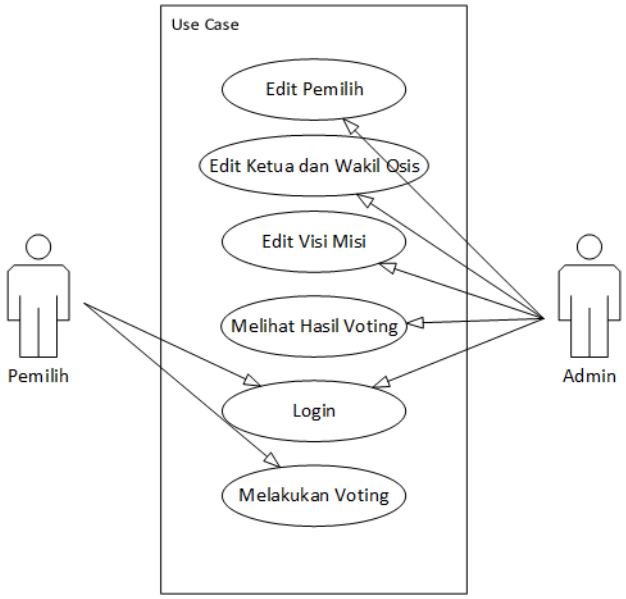
Beberapa hal yang diperlukan dalam desain proses disertakan dengan gambar dan penjelasan sebagai penunjang terkait gambar yang disajikan.

3.6.1 UML

Pada sub bab ini akan dijelaskan tentang workflow(aliran kerja) dari sistem yang berjalan pada perancangan sistem pemilihan ketua dan wakil osis smp 8 palangka raya berbasis web Adapun bentuk pemodelan menggunakan UML. Adapun aktivitas yang terjadi pada sistem ini ialah seperti di bawah ini

3.6.2 Use Case

Berikut ini akan dijelaskan bagaimana Use Case yang terjadi dalam perangkat lunak perancangan sistem e-voting berbasis web yang dimodelkan dalam sekumpulan Use Case dan Actor dan bagaimana hubungan–hubungannya yang akan dipetakan dalam diagram Use Case.

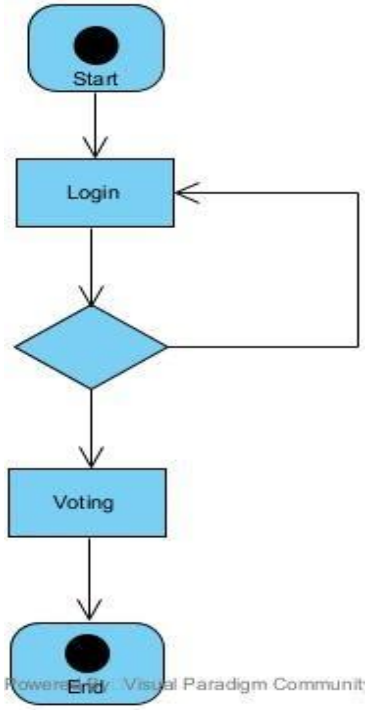


Gambar 3.1 Use Case Diagram Perancangan Sistem Pemilihan Ketua Osis

3.6.3 Activity Diagram

Pada sub bab ini akan dijelaskan tentang workflow(aliran kerja) dari sistem yang berjalan pada perancangan sistem pemilihan ketua dan wakil osis smp 8 palangka raya berbasis web Adapun bentuk pemodelan menggunakan activity diagram. Adapun aktivitas yang terjadi pada sistem ini ialah seperti gambar-gambar di bawah ini :

3.6.4 Activity Diagram Login



Gambar 3.2 Activity Diagram Login

Pada aktifitas pemungutan suara pemilih melakukan beberapa kegiatan untuk melakukan kegiatan pemberian hak suara diantaranya adalah:

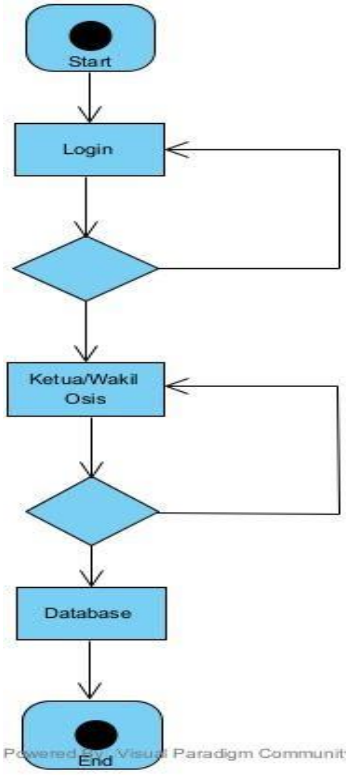
1. Pemilih memilih menu login

2. Kemudian melakukan validasi dengan memasukan username dan password

3. Jika username dan password benar maka akan bisa masuk

4. Jika username dan password salah maka akan ditolak dan tidak bisa masuk system

3.6.5. Activity Diagram Pemilihan Ketua dan Wakil Osis



Gambar 3.3 activity diagram pemilihan ketua dan wakil osis

Pada aktifitas pemungutan suara pemilihan Ketua dan Wakil Osis melakukan beberapa kegiatan untuk melakukan kegiatan pemberian hak suara diantaranya adalah:

1. Pemilih berada pada posisi form login

2. Pemilih menginputkan username dan password

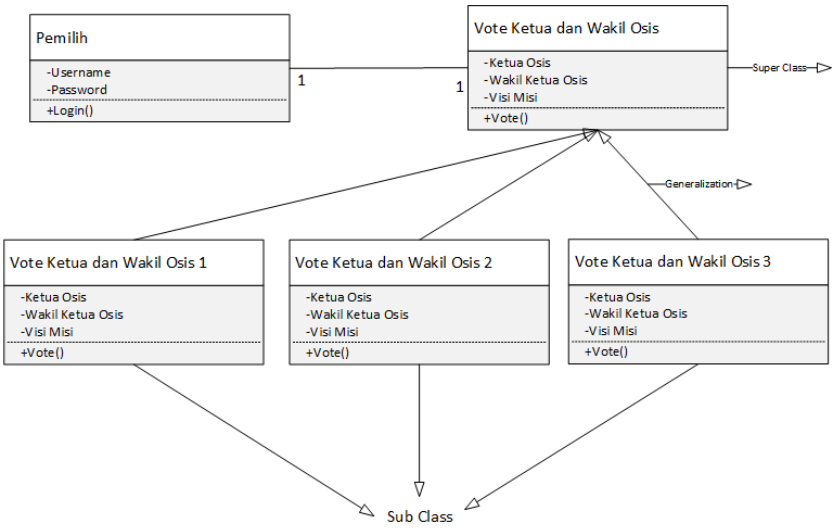
3. Jika data telah dimasukan terus dilakukan validasi data jika benar maka akan melakukan voting Ketua dan Wakil Osis

4. Jika salah maka akan kembali ke form login

5. Jika voting telah dilakukan dengan benar maka simpan ke database

3.6.6 Class Diagram

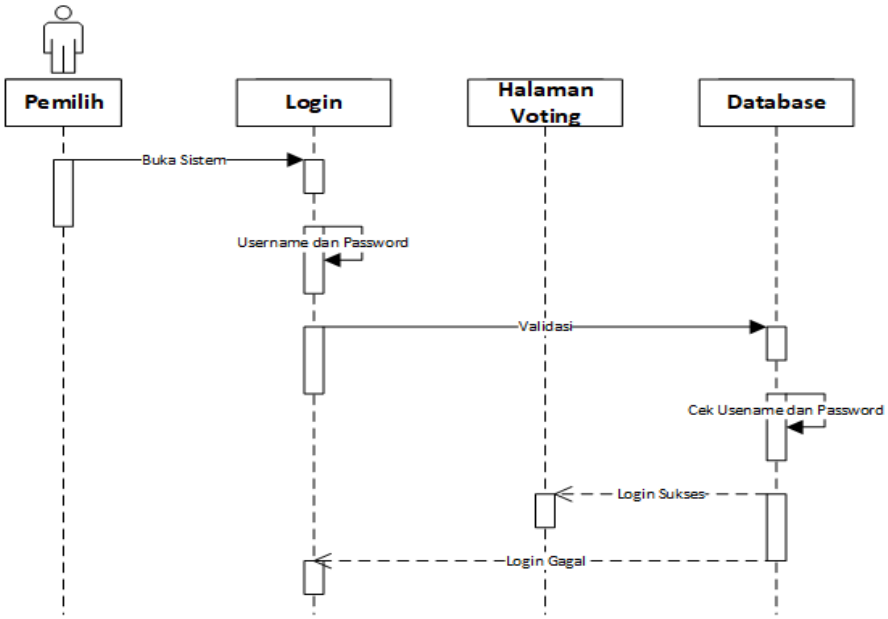
Pada sub bab berikut ini akan dijelaskan bagaimana memodelkan data dalam bentuk Class diagram yang menunjukan sekumpulan class object, antarmuka (interface) dan relasinya, Class yang terdapat dalam perangkat lunak ini terdiri dari class seperti pada gambar berikut ini.



Gambar 3.4 Class diagram perancangan sistem pemilihan ketua osis

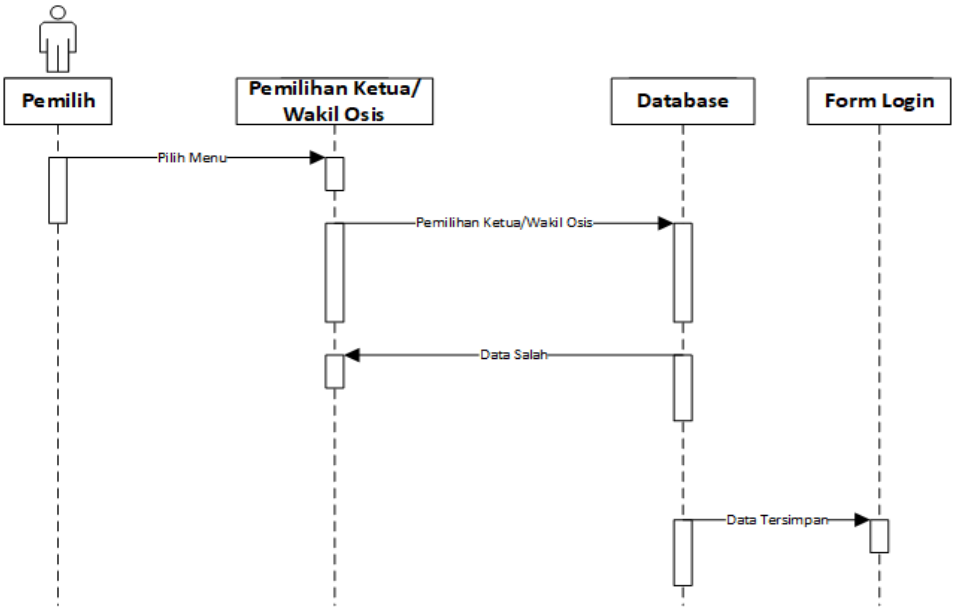
3.6.7 Sequence Diagram

Pada sub bab berikut ini akan digambarkan Sequence diagram yang terbentuk dari class dan objek-objek yang ada seperti Dan berikut ini sequence diagram yang terdapat dalam sistem.



Gambar 3.5 sequence diagram Login

1. Pemilih memasukan username dan password
2. Sistem memeriksa username dan password
3. Jika username dan password benar maka akan masuk ke halaman voting
4. Jika salah username dan password maka akan kembali ke halaman login



Gambar 3.6 Sequence diagram pemilihan ketua osis

1. Pemilih memilih menu pemungutan suara Ketua dan Wakil Osis
2. Sistem menampilkan form pemilihan Ketua dan Wakil Osis
3. Jika telah memilih maka data akan disimpan
4. Jika data salah maka akan kembali memilih ketua osis dan wakil osis

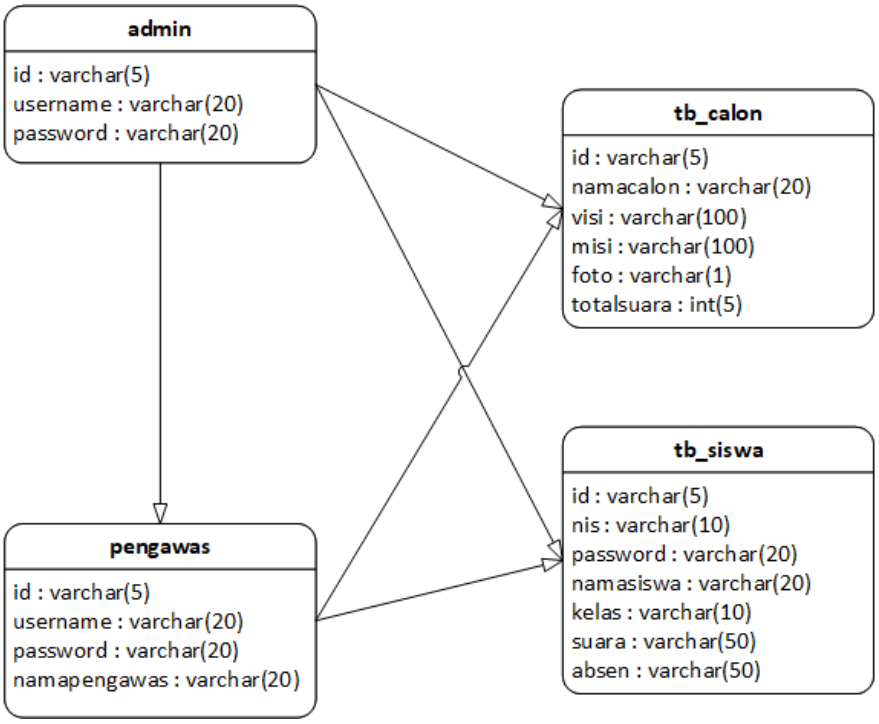
3.7 Class Diagram

- Admin

  Admin bisa melihat, mengedit dan mengelola data di database

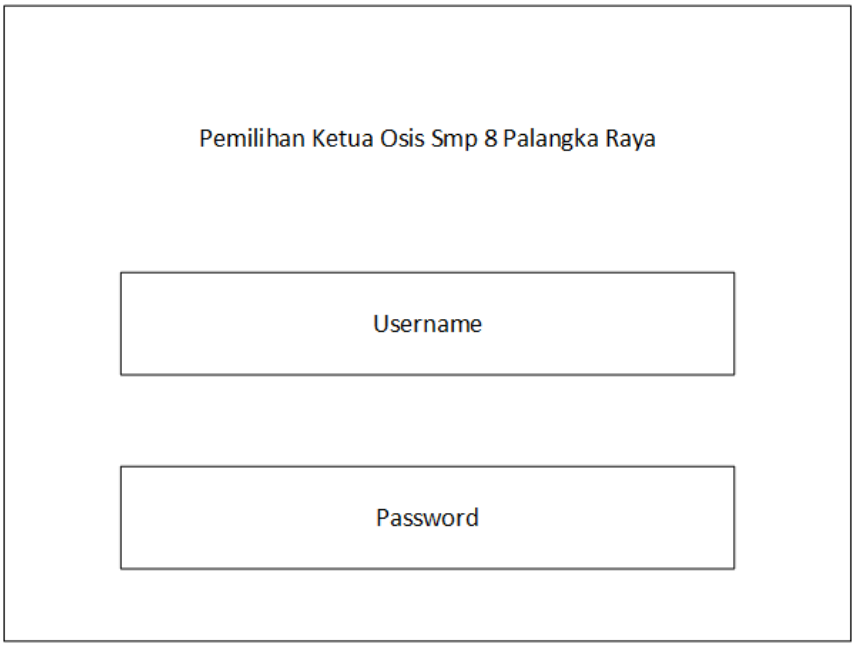
- pengawas

  pengawas hanya bisa melihat orang yang memilih dan hasil pemilihan

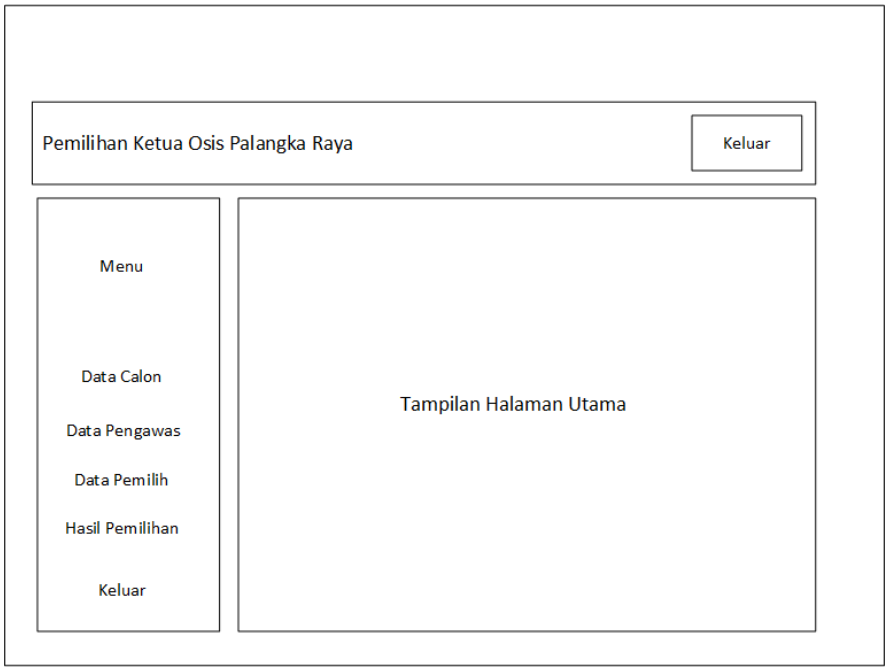


Gambar 3.7 Class Diagram

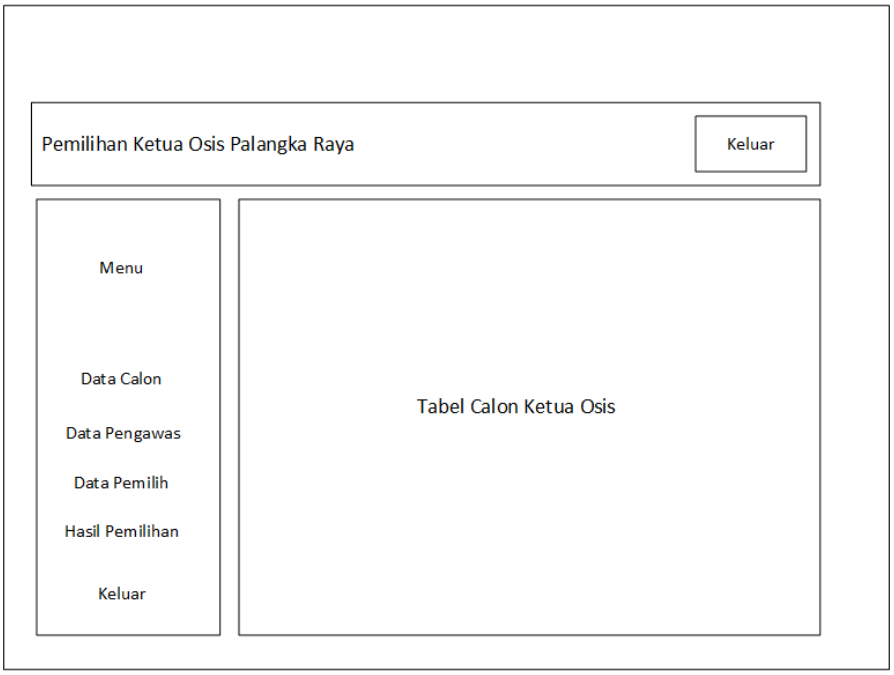
3.8 User Interface



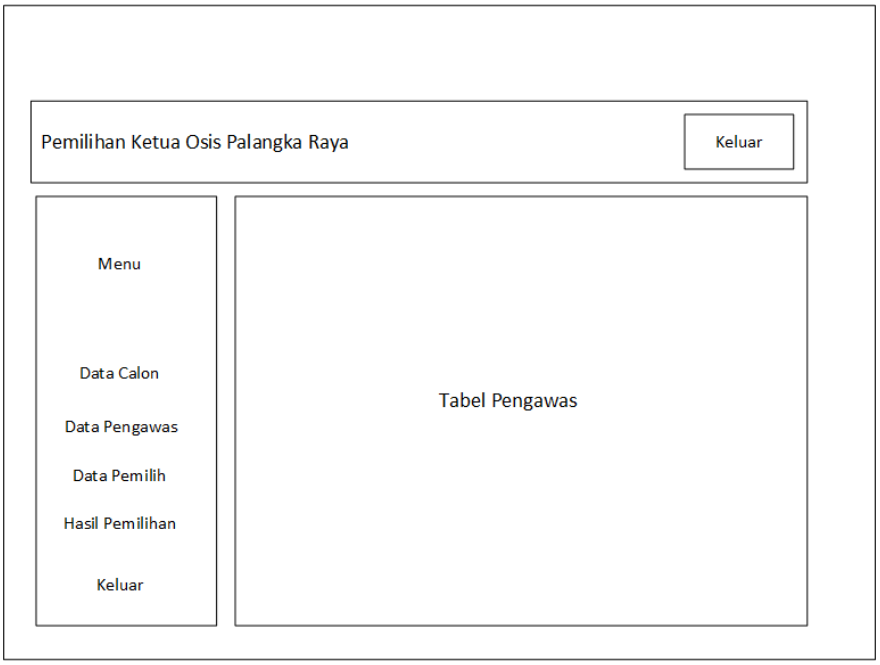
Gambar 3.8 User Interface Login



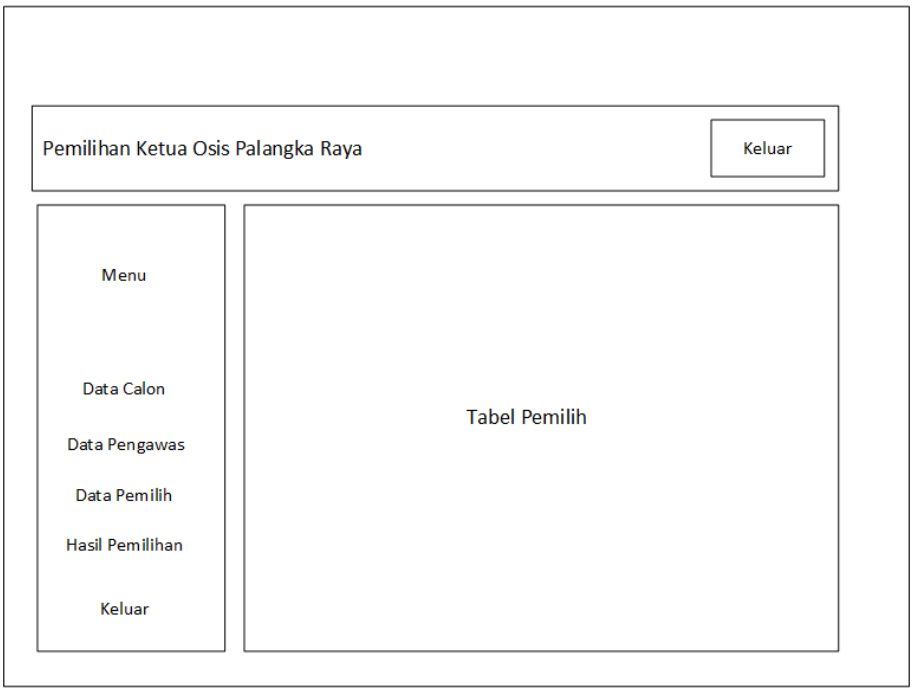
Gambar 3.9 User Interface Halaman Utama



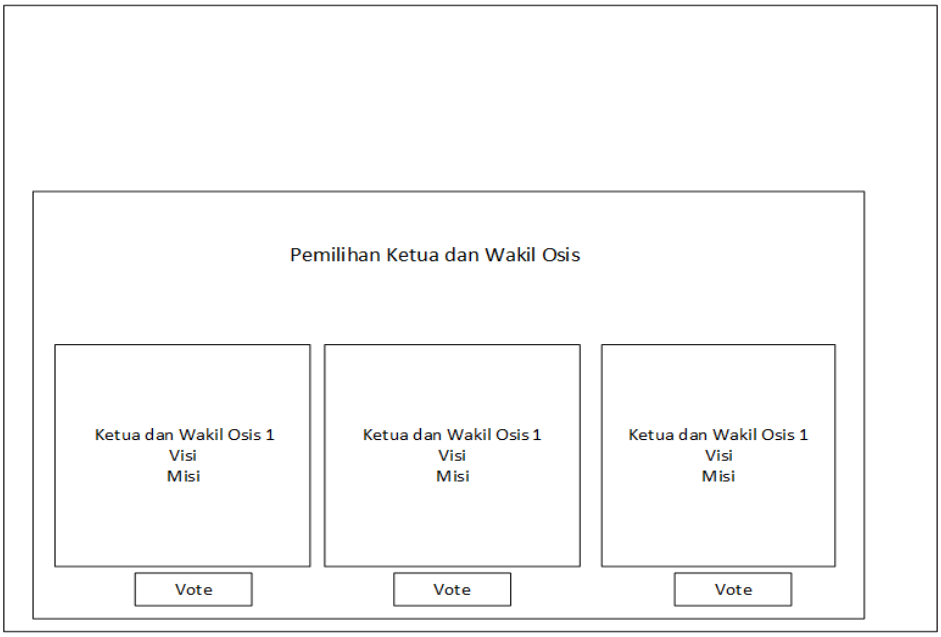
Gambar 4.0 User Interface Data Calon Ketua Osis



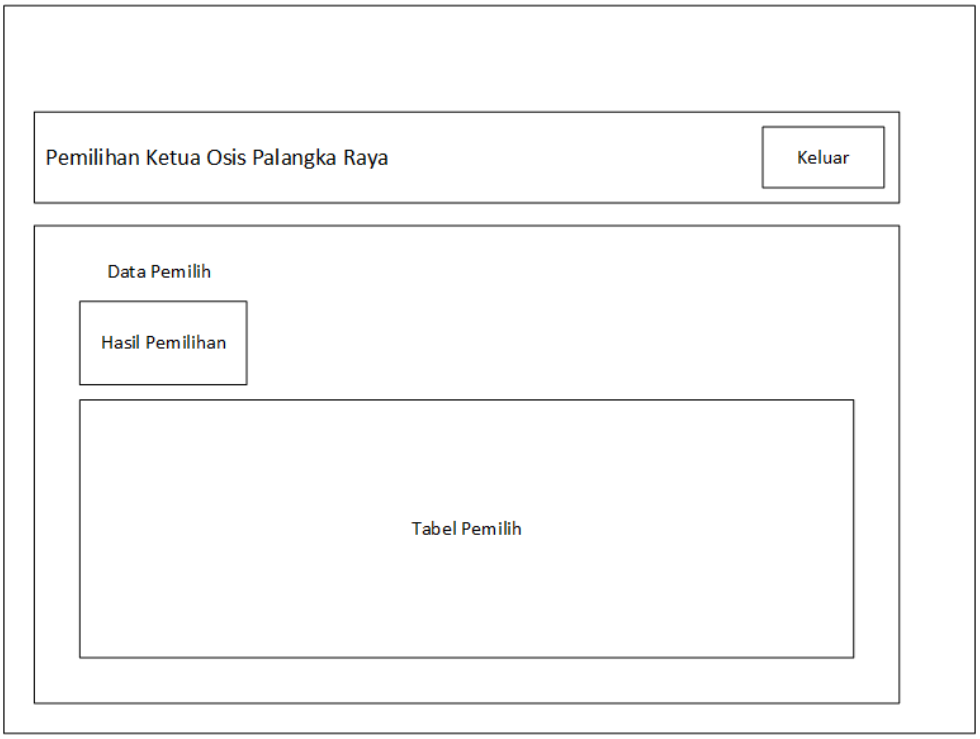
Gambar 4.1 User Interface Data Pengawas



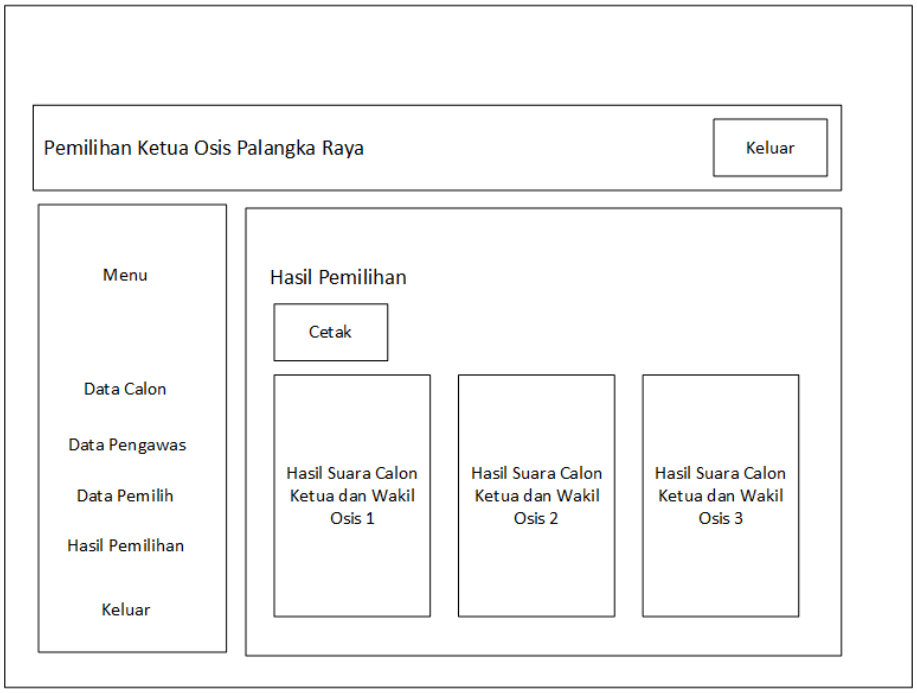
Gambar 4.2 User Interface Data Pemilih



Gambar 4.3 User Interface Voting Ketua dan Wakil Osis



Gambar 4.4 User Interface Pengawas



Gambar 4.5 User Interface Hasil Pemilihan Ketua dan Wakil Osis

BAB IV

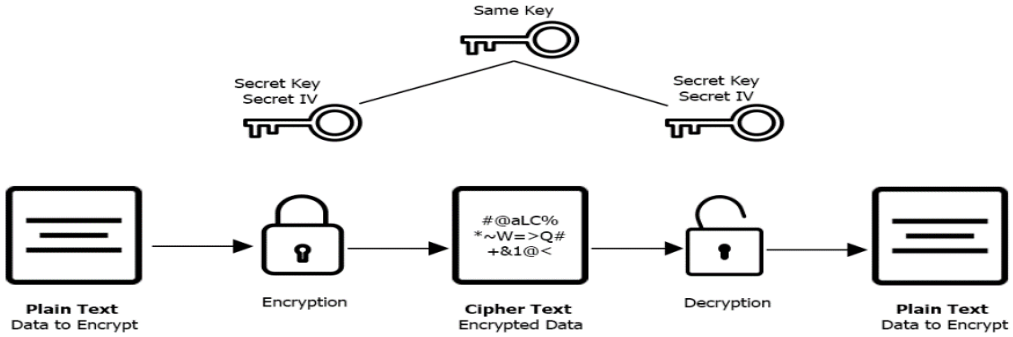
IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi

Setelah melakukan perancangan, langkah selanjutnya yang dilakukan adalah tahap implementasi sistem yang merupakan tahap agar sistem siap dioperasikan. Penjelasan meliputi cara, langkah-langkah serta rencana jadwal pelaksanaan penerapan sistem yang baru. Rencana penerapan ini juga menjelaskan tentang aktifitas-aktifitas yang akan dilakukan dengan penjelasannya.Pengujian .

1. Pembahasan Penerapan AES

Penerapan Algoritma AES untuk keamanan data pemilihan ketua osis pada web server. Penelitian ini bertujuan untuk membangun dan mengimplementasikan sistem keamanan data lapas pada web server menggunakan bahasa pemograman PHP. Hasil dari penelitian ini adalah membangun suatu aplikasi untuk melindungi data pemilih, admin, pengawas dan calon dengan menggunakan algoritma AES secara offline.



Gambar 4.6 Cara Kerja AES

2. Implementasi Antar Muka

Untuk dapat melakukan percobaan pada prototife yang dibuat harus dimulai dengan beberapa istalasi software pendukung yaitu diantaranya :

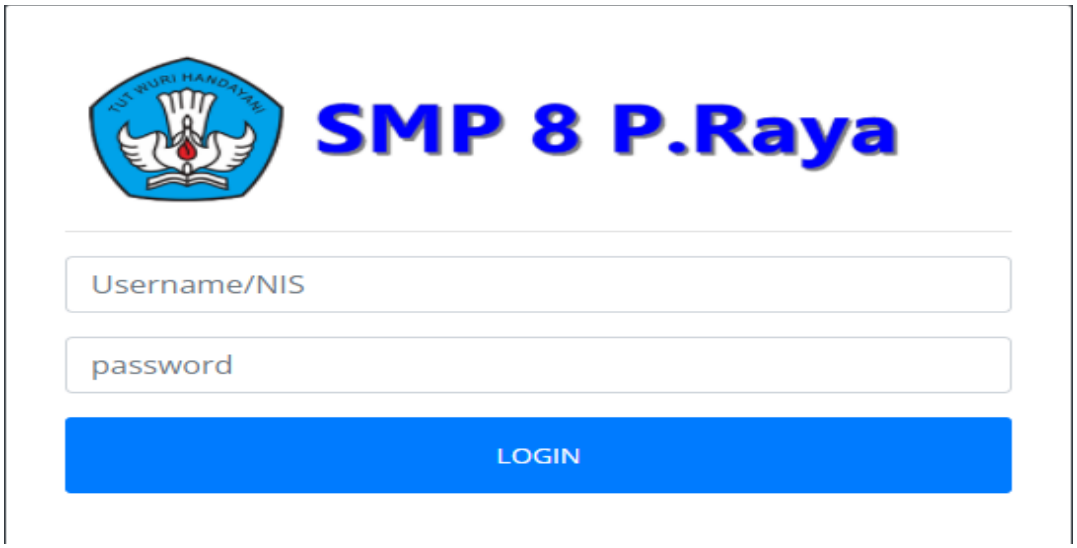
1. Internet Browser (Mozilla,Internet Explorer,google chrome, dll)
2. Instalasi mysql server.
3. Instalasi web server (Apache)

Nama Dialog Screen : Login

Fungsi : untuk melakukan login

Bentuk : -

Keterangan : Gambar 4.7 adalah tampilan untuk halaman login



Gambar 4.7 Login

Petunjuk umum penggunaan program :

1. Pada internet browser ketikan URL localhost

2. Secara otomatis dialog login akan tampil pada web browser sebagai halaman pembuka

3. Didalam halaman login digunakan untuk validasi data pemilih.

4. Masukan username dan password yang benar dan anda bisa melakukan proses pemilihan.

Nama Dialog Screen : Form Pemilihan

Fungsi : untuk melakukan pemilihan ketua dan wakil osis

Bentuk : -

Keterangan : Gambar 4.8 adalah tampilan untuk halaman pemilihan



Gambar 4.8 Pemilihan

Petunjuk umum penggunaan program :

1. Setelah melakukan login Secara otomatis form ini akan tampi

2. Pemilih melakukan pemilihan Ketua dan Wakil Osis

Nama Dialog Screen : Voting

Fungsi : voting ketua dan wakil osis

Bentuk : -

Keterangan : Gambar 4.9 adalah tampilan untuk halaman voting



Gambar 4.9 Voting

Petunjuk umum penggunaan program :

1. Setelah melihat visi dan misi ketua osis

2. Pemilih menekan pilih Ketua dan Wakil Osis

3. Pengujian Blackbox

Bentuk pengujian menggunakan metode Black-Box berfokus pada persyaratan fungsional perangkat lunak. Dengan demikian, pengujian black-box memungkinkan perekayasa perangkat lunak mendapatkan serangkaian kondisi input yang sepenuhnya menggunakan semua persyaratan fungsional untuk suatu program. pengujian black-box berusaha menemukan kesalahan dalam kategori sebagai berikut :

1. Fungsi-fungsi yang tidak benar atau hilang

2. Kesalahan interface

3. Kesalahan dalam struktur data atau akses database eksternal

4. Kesalahan kinerja

5. Inisialisasi dan kesalahan terminasi.

4. Skenario pengujian

Pada skenario pengujian ini akan di jelaskan tentang pengujian yang dilakukan pada perangkat lunak seperti yang akan di jelaskan pada table skenario pengujian berikut ini.

Table 4.1 Skenario Pengujian Login

No	Fungsi yang diuji	Cara Pengujian	Hasil Yang diharapkan	HasilPengujian
1	Verifikasi Login	Tekan tombol logi	Verifikasi username dan password ketika login	Baik
2	Login satu kali	Tekan Tombol login	Ketika pemilih sudah memilih maka akan muncul pesan peringatan	Baik

Table 4.2 Skenario Pengujian Proses Voting

No	Fungsi yang diuji	Cara Pengujian	Hasil Yang diharapkan	HasilPengujian
1	Proses Voting	Tekan tombol Vote	Data Tersimpan ke database	Baik

Table 4.3 Skenario Pengujian Proses Cetak Laporan

No	Fungsi yang diuji	Cara Pengujian	Hasil Yang diharapkan	HasilPengujian
1	Proses Cetak Laporan	Tekan tombol cetak	Data akan tercetak	Baik

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

1. Diharapkan dengan adanya aplikasi ini pemilihan umum dapat berjalan dengan jujur dan adil serta bisa meminimalisir kesalahan yang dapat dilakukan oleh manusia atau dan mengurangi manipulasi dan kecurangan yang bisa terjadi.

2. Dengan adanya aplikasi ini diharapkan dapat membantu siswa dan guru dalam melakukan kegiatan pemilihan ketua osis yang jujur dan adil dan terbebas dari kecurangan.

3. Aplikasi ini diharapkan bisa memberikan layanan yang memuaskan bagi siswa/guru dan bisa menjadikan proses pemilihan yang jujur adil dan rahasia serta terbebas dari kecurangan dan manipulasi hasil pemilihan.

5.2. Saran

1. Harus segera dibuat domain untuk bias mengakses aplikasi melalui website,.

2. Harus segera dibuatkan e voting yang bisa di akses melalui perangkat mobile agar dapat mempermudah siswa dan guru dalam melakukan kegiatan pemilihan tetapi tetap tidak menghilangkan peraturan yang langsung umum bebas dan rahasia.

DAFTAR PUSTAKA

M, Muzakki. Mukhtar., 2016. Simulasi E-Voting Untuk Pemilihan Ketua Himpunan Mahasiswa Jurusan (HMJ) Berbasis Multimedia Home Platform. p. 93.

Ressa, 2019. Sistem Electronic Voting (E-Voting) Berbasis Web Pada Pemilihan Ketua Osis. p. 41.

Subhan, D., 2012. Sistem E-Voting Berbasis Web. p. 108.

Yulianto Agus, Y. H. D. F., 2019. Penerapan E-Voting Dengan Metode Waterfall Untuk Pemilihan Ketua Osis Pada SMP PGRI Parung Panjang Bogor. p. 8.