P-ISSN: 2548-1932
e-ISSN: 2549-7758

SISTEM KEAMANAN JARINGAN DALAM UJIAN ONLINE SMA/SMK MENGGUNAKAN METODE ALGORITMA *ADVANCED ENCRYPTION STANDARD (AES)*

Gylang Satria Yudha[1], Riffa Haviani Laluma[2]

[1,2]Program Studi Teknik Informatika
Universitas Sangga Buana
gylangsatriayudha@outlook.com[1], rhaviani@gmail.com[2]

ABSTRAK

Pada era modernisasi ini, ketika perkembangan zaman sudah memasuki Industri 4.0, penggunaan teknologi sudah semakin berkembang dengan pesat, dari berbagai sektor sudah menggunakan teknologi sebagai media penunjang keseharian, baik itu dalam bidang kesehatan, militer dan bahkan pendidikan, salah satu pemanfaatan teknologi dalam bidang Pendidikan adalah penerapan ujian *online* sebagai media pembelajaran, namun dibalik praktisnya media ujian *online* tersebut, masih ditemukan banyak celah dalam sektor keamanan, dan dengan itu, dibutuhkannya sebuah *system* ujian *online* dengan menerapkan *system* keamanan yang mampu memberikan pengamanan yang efektif dan akurat, salah satu hal yang mampu menutupi celah tersebut adalah dengan menerapkan sebuah metode algoritma enkripsi *Advanced Encryptions Standard* yang saat ini masih menjadi salah satu enkripsi populer paling banyak digunakan, berdasarkan hasil penelitian ini penerapan metode algoritma *Advanced Encryptions Standard* mampu melakukan enkripsi data pada komponen penting ujian *online* seperti *password*, soal dan jawaban dengan mengubah dan mengolah *plaintext* menjadi nilai hash menggunakan *private key* sehingga menghasilkan *chipertext.*

Kata Kunci: *AES, Algoritma Kunci Simetris, Enkripsi, MySQL.*

1. PENDAHULUAN

Pada era moderenisasi ini penggunaan teknologi sudah semakin berkembang, hampir setiap aktifitas manusia dilakukan secara terkomputerisasi, yang mana fungsi komputer tidak hanya sebagai alat penghitung saja. Semejak masuk kedalam industri 4.0, fungsi komputer sudah menjadi perangkat dan media yang menjadi solusi untuk pemecahan masalah yang banyak dihadapi manusia. Penggunaan teknologi selain menjadi perangkat untuk membantu sektor bisnis, juga menjadi perangkat yang membantu pada sektor Pendidikan, karena teknologi Pendidikan itu sendiri merupakan pengembangan, penerapan dan penilaian sistem-sistem, teknik dan alat bantu untuk meningkatkan proses belajar manusia [1]. Selain itu teknologi Pendidikan juga merupakan proses yang kompleks, terpadu yang melibatkan orang, prosedur, ide, peralatan, dan organisasi demi menganalisis masalah dan mencari jalan pemecahannya, melaksakan, mengevaluasi dan mengelola pemecahan masalah yang menyangkut semua aspek belajar manusia [2].

Dalam teknologi Pendidikan, paling umum adalah untuk menerapkan sistem informasi yang berkaitan dengan masalah internal instansi, termasuk didalamnya adalah ujian online yang saat ini sudah banyak diterapkan dihampir setiap sekolah diseluruh Indonesia. Ujian online merupakan proses pelaksanaan ujian yang dilakukan secara *real-time* melalui komputer, *tablet,* dan *smartphone* yang terhubung dengan sambungan *internet*. Dengan adanya ujian *online*, proses belajar dan pelaksanaan ujian bisa dilaksanakan secara efisien darimanapun tanpa memandang tempat dan waktu, sehingga sangat cocok digunakan bagi siswa yang sedang berada diluar sekolah

P-ISSN: 2548-1932
e-ISSN: 2549-7758

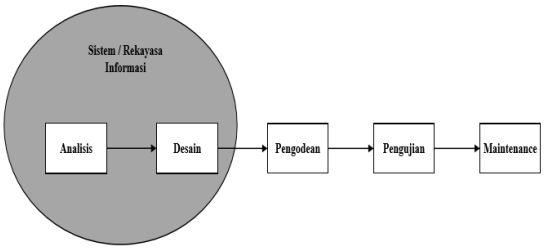
akibat kendala atau sedang ada keperluan yang mengharuskan siswa tidak dapat menghadiri pembelajaran pada saat itu. Namun dengan ujian *online*, tidak dapat dipungkiri bahwa masih banyak kekurangan yang bisa mengakibatkan kecurangan dan pencurian data dalam proses dan pelaksanaan ujian *online*, sehingga dengan hal ini perlu diterapkan sebuah sistem keamanan yang mampu meminimalisir kecurangan dan pencurian data yang terjadi, karena sistem keamanan komputer dan jaringan adalah sesuatu yang berhubungan dengan pencegahan diri dan deteksi terhadap sebuah atau beberapa tindakan pengganggu yang tidak dikenali dalam sistem komputer[3], selain itu keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan *illegal* yang tidak bertanggung jawab[4].

Oleh karena itu dengan menerapkan sistem keamanan pada komputer untuk melakukan pengamanan data yang bersifat sensitif terutama dalam proses ujian *online*, diperlukan metode enkripsi dan algoritma kriptografi yang kuat demi mendukung masalah tersebut, dan *Advanced Encryption Standard (AES)*, menjadi salah satu metode algoritma paling popular dan diakui keamanannya hingga saat ini, *Advanced Encryption Standard (AES)* merupakan salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetrik[5].

2. TINJAUAN PUSTAKA

2.1. Model Pengembangan Perangkat Lunak

Metode pengembangan perangkat lunak yang digunakan dalam penelitian ini menggunakan *System Development Life Cycle SDLC)* dengan menggunakan model *waterfall. System Development Life Cycle* merupakan salah satu metode pengembangan sistem yang saat ini populer digunakan pada sistem informasi ketika pertama kali dikembangkan[6]. Sedangkan model *waterfall* merupakan model yang cocok untuk pengembangan dengan spesifikasi yang tidak berubah ubah[6].



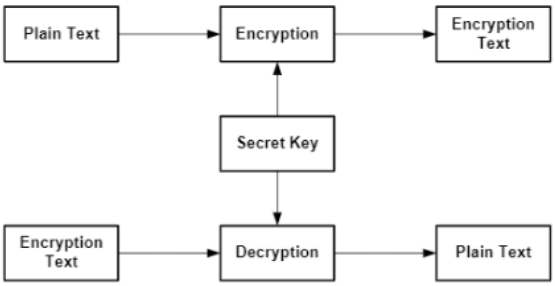
Gambar 1 Model Waterfall Menurut Rosa dan Salahudin

2.2. Metode Enkripsi

Salah satu hal penting dalam keamanan jaringan yang menggunakan komputer terutama dalam hal komunikasi adalah untuk menjamin kerahasiaan data yang dikirimkan, dengan itu munculah sebuah metode enkripsi dalam pengamanan suatu data. Enkripsi yaitu suatu proses pengamanan sebuah data yang disembunyikan atau dilakukannya sebuah proses konversi data (plaintext) menjadi bentuk yang tidak dapat dibaca dan dimengerti (*chipertext*). [5]

2.3. Algoritma Simetrik

Algoritma simetris biasanya disebut sebagai algoritma kunci rahasia (*private key*). Dalam algoritma simetris enkripsi dapat dilakukan jika pengirim informasi dan penerimanya telah sepakat untuk menggunakan sebuah metode enkripsi atau kunci rahasia (*secret key*) dari sebuah enkripsi tertentu. Proses enkripsi dan dekripsi dalam algoritma simetris ini menggunakan satu kunci rahasia (*secret key*) yang telah disepakati sebelumnya. [7]



Gambar 2 Algoritma Simetris

2.4. Algoritma *Advanced Encryption Standard (AES)*

Dari sekian banyaknya metode enkripsi, algoritma *Advanced Encryption Standard* (AES) lah yang saat ini paling populer digunakan dalam berbagai sektor keamanan. *Advanced Encryption Standard* (AES)

P-ISSN: 2548-1932
e-ISSN: 2549-7758

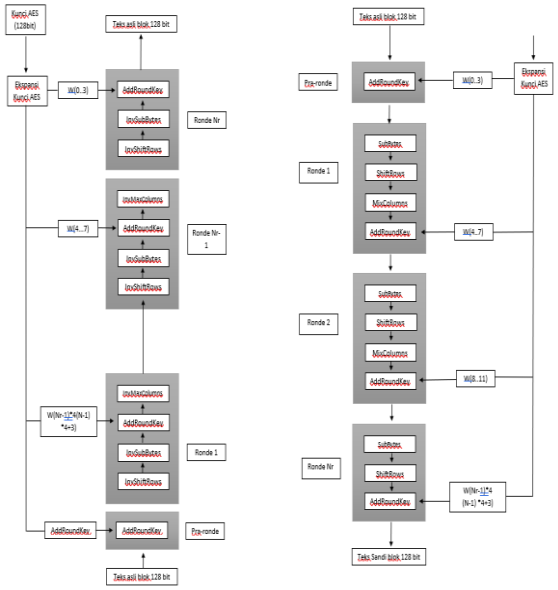
merupakan sebuah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris pada saat ini. Didalam algoritma kriptografi AES 128, 1blok plainteks berukuran 128 bit terlebih dahulu dikonversi menjadi matriks heksadesimal berukuran 4x4 yang disebut state. Setiap elemen state berukuran 1 byte. Proses enkripsi pada AES merupakan transformasi terhadap state secara berulang dalam 10 ronde. [8]

Advanced Encryption Standard juga, biasanya disebut sebagai sebuah sistem penyandian blok yang bersifat non-feistel karena AES menggunakan komponen yang selalu memiliki invers dengan Panjang blok 128 bit, kunci AES juga menggunakan proses yang berulang yang disebut dengan *round*, Proses didalam algoritma juga AES merupakan transformasi terhadap *state*. Sebuah teks asli dalam blok (128 bit) terlebih dahulu diorganisir sebagai *state*. Enkripsi AES menggunakan transformasi terhadap *state* secara berulang dalam beberapa *ronde*. State yang menjadi keluaran ronde k menjadi masukan untuk ronde ke-k +1.

Pada proses enkripsi awalnya teks asli dibentuk sebagai sebuah state, dan kemudian sebelum ronde 1 dimulai blok teks asli dicampur dengan kunci ronde ke-0 (transformasi ini juga disebut sebagai *AddRoundKey*), selanjutnya setelah itu, ronde ke-1 sampai dengan ronde ke-(Nr-1) yang mana Nr adalah jumlah ronde. AES menggunakan 4 jenis transformasi yaitu:

1. SubBytes, sebagai proses transformasi subtutusi.
2. ShiftRows, sebagai proses transformasi permutasi.
3. MixColumns, sebagai proses transformasi pengacakan.
4. AddRoundKey, sebagai proses transformasi penambahan kunci.

Pada ronde terakhir, yaitu ronde ke-Nr dilakukan transformasi serupa dengan ronde lain namun kali ini tanpa transfomasi serupa dengan proses transformasi MixColumns. Algoritma dekripsi AES dapat diilustrasikan seperti Gambar 1.3. Dan secara ringkas algoritma deskripsi merupakan kebalikan dari algoritma enkripsi AES. Algoritma dekripsi AES menggunakan transformasi *invers* semua transformasi dasar yang digunakan pada algoritma enkripsi AES. Setiap tranformasi dasar dari algoritma kriptografi AES memiliki transformasi invers, yaitu: InvSubBytes, InvShiftRows dan InvMixColumns. AddroundKey merupakan transformasi yang bersifat self-invers dengan syarat mengunakan kunci yang sama[10].



Gambar 3. Ilustrasi Enkripsi dan Dekripsi AES

Penyandian AES membutuhkan kunci ronde untuk setiap ronde transformasi kunci, kemudian ronde ini di bangkitkan atau di ekspansi dari kunci AES. Kunci AES 128bit atau 4word menghasilkan sebuah larik sebanyak 44word yang menjadi kunci. Berikut adalah langkah langkah mengekspansi kunci:

1. Pertama kunci AES 128 bit di organisir menjadi 4 word dan disalin ke word keluaran (W) pada 4 elemen pertama (W[0], W[1], W[2], W[3]).
2. Untuk elemen keluaran selanjutnya W[i] dengan i={4,…,43} dihitung sebagai berikut:
   - Salin W [i-1] pada word t.
   - Jika i mod 4 = 0 (I habis dibagi 4) maka lakukan W[i]= f (t,i) ⊕ W[i-4] ,dengan fungsi f(t,i) adalah sebagai berikut:

     f(t,i) = Subword (rotword(t)) ⊕ RC[i/4]

   - Jika I mod 4 tidak sama dengan 0, lakukan W[i]= t ⊕ W[i-4].

P-ISSN: 2548-1932
e-ISSN: 2549-7758

3. Unified Modelling Language (UML)

   Pemodelan yang dilakukan menggunakan *Unified Modelling Language* (UML), yang merupakan Bahasa *visual* untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks pendukung[9]. Berikut merupakan penjelasan mengenai empat diagram Unified Modelling Language (UML) yang digunakan:

   a. Use Case Diagram.

      Use Case Diagram merupakan pemodelan untuk melakukan (behavior) dari sistem informasi yang akan dibuat, Use Case mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibuat[9].

   b. Activity Diagram

      Activity diagram merupakan penggambaran workflow atau alur kerja atau aktifitas dari sebuah sistem atau proses bisnis.

   c. Sequence Diagram.

      Sequence diagram merupakan gambaran tahap demi tahap, termasuk kronologi (urutan) perubahan secara logis yang seharusnya dilakukan untuk menghasilkan sesuai sesuai dengan use case diagram [11].

   d. Class Diagram

   Class diagram merupakan suatu set objek yang memiliki atribut dan perilaku yang sama, class diagram kadang disebut sebagai object diagram[12].

4. Black Box Testing

   Pengujian yang dilakukan dalam penelitian ini menggunakan metode *Black Box* yang mana, *Black Box Testing* merupakan proses menguji perangkat lunak dari segi spesifikasi fungsional tanpa menguji desain dan kode program. Pengujian dimaksudkan apakah hasil dari masukan dan keluaran yang dihasilkan program sesuai dengan spesifikasi yang dibutuhkan[9].

3. HASIL DAN PEMBAHASAN

Pada tahapan ini, aplikasi ujian *online*, diuji dan diterapkan pada salah satu instansi Pendidikan Sekolah Menengah Kejuruan Bina Anak Bangsa, menghasilkan beberapa tahapan dalam pembahasan yang diantaranya adalah:

3.1. Tahapan Analisis

Perancangan aplikasi yang akan digunakan sebagai media ujian online dengan penerapan metode Advanced Encryption Standard (AES), menggunakan beberapa komponen yang diantaranya.

1. Apache Web Server

   Apache HTTP *server* adalah perangkat lunak dengan *platform operating system* (OS) yang mendukung *multi-tasking*, dan menyediakan layanan untuk aplikasi lain yang terhubung ke dalamnya, seperti *web browser*. Apache pertama kali dikembangkan untuk bekerja dengan sistem operasi *Linux/Unix*, tetapi kemudian diadaptasi untuk bekerja di bawah sistem lain, termasuk Windows dan Mac [13].

2. Database MySQL.

   Salah satu media paling penting untuk menerapkan sistem keamanan jaringan pada proses pengamanan data ujian online adalah dengan menggunakan database MySQL. MySQL merupakan sebuah *database* yang mengandung satu atau beberapa tabel. [8].

3. Framework Codeigniter

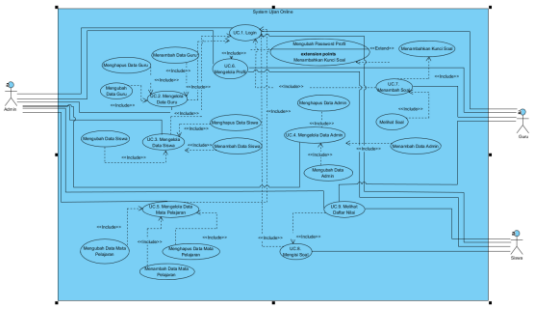
   Pada aplikasi ujian *online* yang dibuat, dibangun diatas *framework* codeigniter. Codeigniter sendiri merupakan sebuah *web application framework* yang digunakan untuk membangun aplikasi PHP dinamis yang dibangun menggunakan konsep *Model View Controller development pattern.* CodeIgniter menyediakan berbagai macam *library* yang dapat mempermudah dalam pengembangan dan termasuk framework tercepat dibandingkan dengan *framework* lainnya.[15]

P-ISSN: 2548-1932
e-ISSN: 2549-7758

3.2. Desain

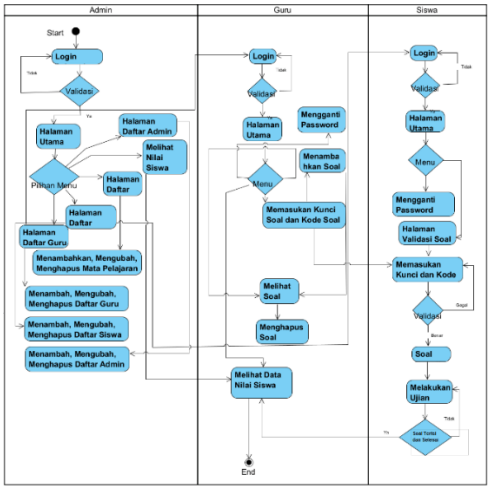
Proses desain sistem menggunakan *Unified Modeling Language (UML)*, yang diantaranya menggunakan *Use Case* Diagram, dan *Activity* Diagram.

1. *Use Case* Diagram.



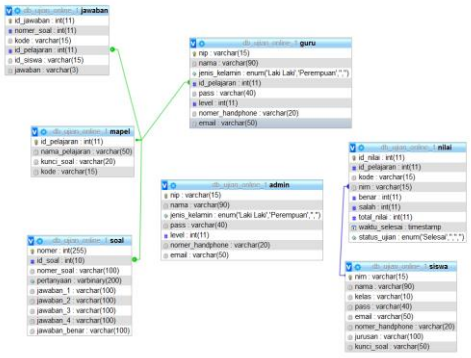
Gambar 4. Use Case Diagram Ujian Online

2. *Activity* Diagram



Gambar 5. Activity Diagram Rancangan Desain Ujian Online

3. Desain Basis Data



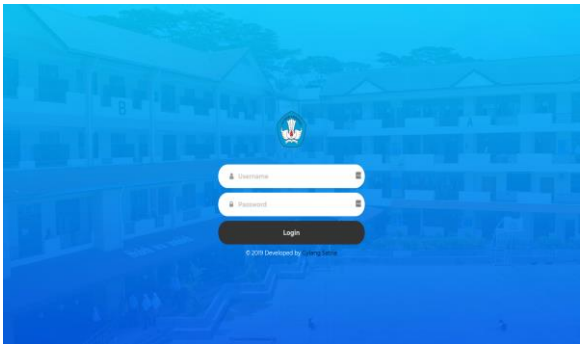
Gambar 6. Desain Basis Data

3.3. Implementasi Metode

Implementasi metode algoritma AES, diterapkan pada komponen penting dari system itu sendiri, diantaranya (password akun, soal ujian, dan jawaban ujian), dengan mengubah teks asli menjadi teks yang acak didalam *Database* MySQL, pengacakan sendiri sudah menggunakan algoritma AES.

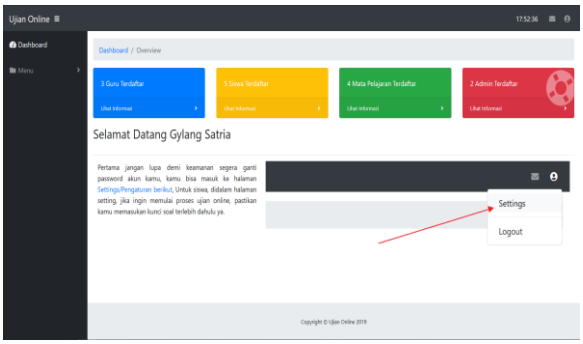
3.4. Tampilan Aplikasi

Berikut adalah tampilan aplikasi ujian online yang telah dibuat.



Gambar 7. Halaman *Login*

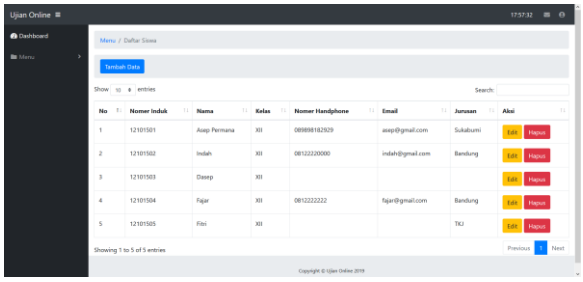
Pada halaman *login*, setiap akses yang mana itu adalah (Guru, Siswa dan Admin) akan masuk kehalaman Login setelah masuk ke alamat ujian *online*.



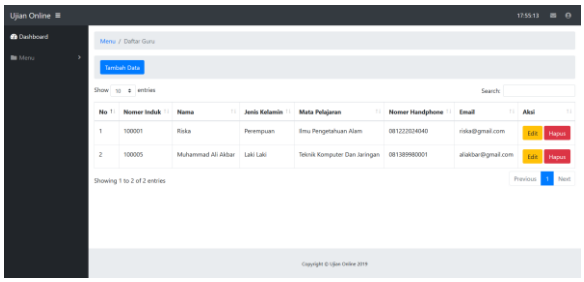
Gambar 8. Halaman Dashboard Admin

Pada halaman ini akan menampilkan beberapa menu dan kontrol penuh mengenai akun yang dapat mengakses aplikasi ujian online, seperti menambah, mengedit dan menghapus akun (admin, siswa, dan guru) serta data (mata pelajaran). Pada akses admin pun bisa melihat daftar nilai dari semua siswa dan semua pelajaran tanpa mengubah, dan menghapusnya.

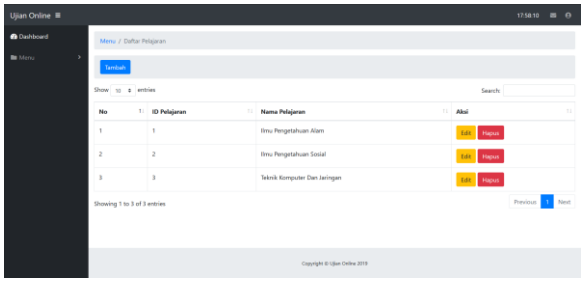
P-ISSN: 2548-1932
e-ISSN: 2549-7758



Gambar 9. Halaman Pengelola Siswa

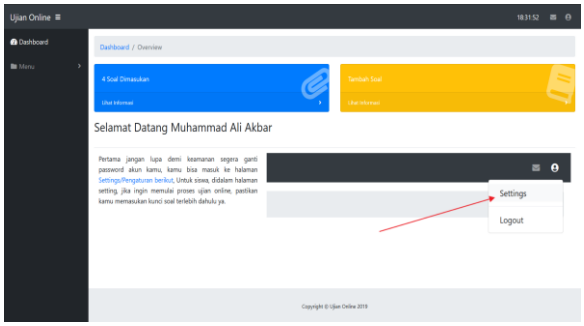


Gambar 10. Halaman Pengelola Siswa

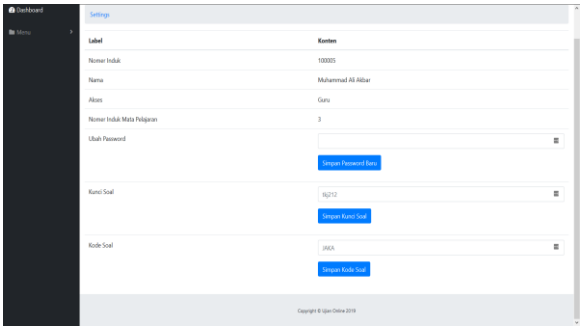


Gambar 11. Halaman pengelola Mata Pelajaran

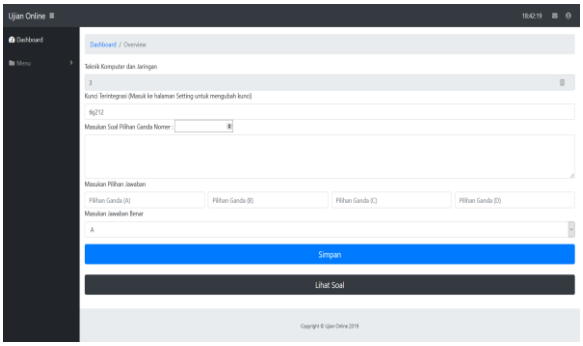
Selanjutnya pada akses guru, diberikan halaman *dashboard* yang serupa dengan admin, namun memiliki akses menu yang berbeda diantaranya (menambahkan, menghapus dan mengubah soal), dan akses khusus untuk menambah, mengubah kunci soal dihalaman profile. Kunci ini juga yang akan melakukan enkripsi dan dekripsi dari soal dan jawaban.



Gambar 12. Halaman *Dashboard* Guru

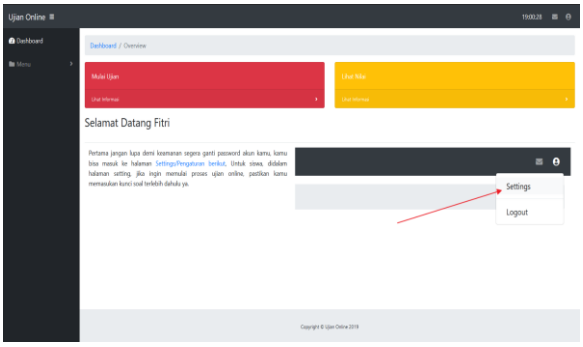


Gambar 13. Halaman Profile Guru

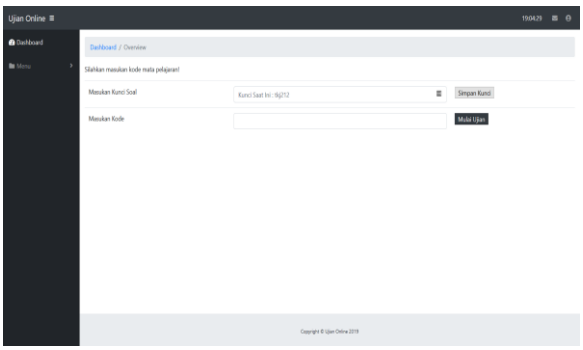


Gambar 14. Halaman Membuat Soal

Selanjutnya pada akses Siswa, siswa diperkenankan untuk mengisi soal, namun sebelum masuk kehalaman pengisian soal, siswa diharuskan untuk memasukan kunci soal yang dibuat oleh guru sebelumnya.

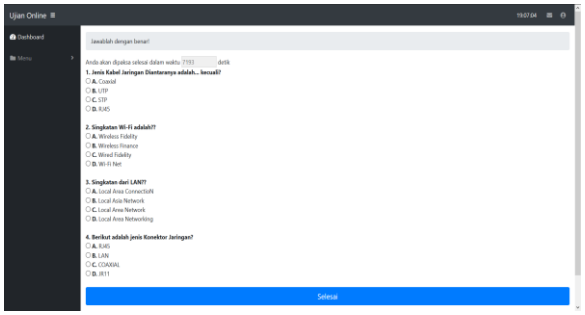


Gambar 15. Halaman Dashboard Siswa

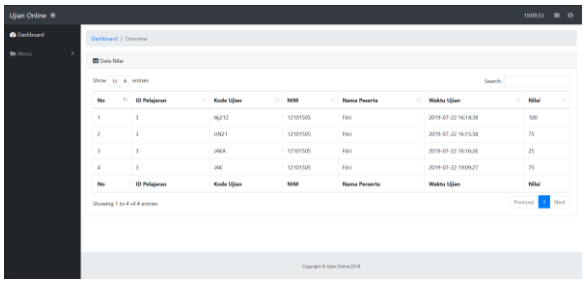


Gambar 16. Halaman Validasi Soal

P-ISSN: 2548-1932
e-ISSN: 2549-7758



Gambar 17. Halaman Pengisian Soal



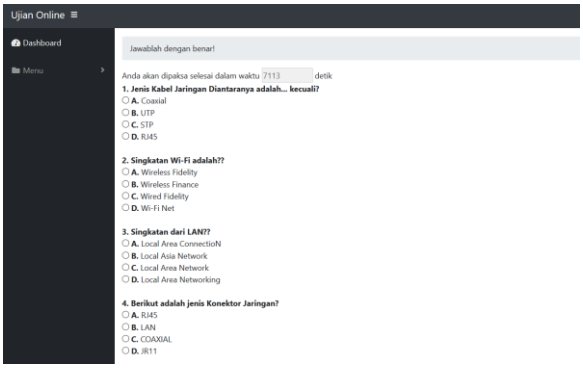
Gambar 18. Halaman Daftar Nilai

Pada halaman daftar nilai, setiap user diberikan akses melihat daftar nilai siswa, untuk admin bisa melihat seluruh nilai dari seluruh pelajaran, guru melihat seluruh nilai siswa dari pelajaran yang sesuai dengan mata pelajaran guru, dan siswa bisa melihat daftar nilai sesuai dengan akun miliknya.

3.5. Pengujian Keamanan

Pada pengujian ini dilakukan dengan pengecekan memasukan kunci soal secara benar dan salah, pertama, ketika siswa gagal atau salah memasukan kunci soal pada halaman validasi, maka siswa tidak akan bisa mengisi soal dikarenakan halaman akan kosong dan acak.

Gambar 19. Halaman Soal (Salah)



Gambar 20. Halaman Soal (Benar)

Selanjutnya pengujian dilakukan menggunakan skenario, seandainya ada pihak asing yang berhasil masuk kedalam database dan berniat mencuri kunci jawaban.

Gambar 21. Skenario Pengujian Pencurian Kunci Jawaban.

4. KESIMPULAN

Berdasarkan hasil implementasi dan pengujian sistem, penulis dapat memperoleh kesimpulan yang dapat diambil dari penelitian mengenai Sistem Keamanan Jaringan Dalam Ujian Online SMK/SMA Menggunakan Metode Algoritma *Advanced Encryption Standard* (AES) sebagai berikut:

1. Hasil dari penelitian ini menunjukan bahwa sistem keamanan jaringan pada aplikasi ujian online, mampu mengamankan soal dan jawaban yang tersimpan dalam database, baik dari pihak dalam, ataupun luar.
2. Penerapan ujian online yang diterapkan, mampu menekan biaya ujian, dari konvensional menjadi berbasis teknologi.

DAFTAR PUSTAKA

[1] Nasution, S. (1987). Teknologi Pendidikan. Bandung: Jemarrs.
[2] Miarso, Y. (1986). Definisi Teknologi Pembelajaran; Satuan Tugas dan Terminologi. Jakarta: Rajawali Press.
[3] Gollman, D. (1999). Computer Security. Chichester, UK: A John Wiley and Sons Ltd.
[4] Howard, J. D. (1997). An Analysis of Security Incidents on The Internet. Pittsburgh: CARNEGIE MELLON UNIVERSITY.
[5] Rijmen, D. (1998). AES submission document on Rijndael.
[6] Rosa, A. S., & Shalahuddin, M. (2013). Rekayasa Perangkat Lunak. Bandung: Informatika.
[7] Sugeng, M. (2014). Mengenal Perhitungan Enkripsi Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES) Rijndael: Infokam.
[8] Tulloh, A. R., Permanasari, Y., & Harahap, E. (2016). Kriptografi Advanced Encryption Standard (AES) Untuk Penyajian Dokumen. Jurnal Matematika UNISBA, Vol 15 No 1.
[9] A. R., & S. M. (2015). Rekayasa perangkat lunak Terstuktur Dan Berorientasi Objek. Bandung: Informatika.
[10] Stalling, W. (2003). Cryptography and Network Security Principles and Practice. New Jersey: Pearson Education.
[11] Haviluddin. (2011). Memahami Penggunaan UML (Unified Modelling Language). Jurnal Informatika Mulawarman.
[12] Indra Griha Tofik Isa, & George Pri Hartawan. (2017). PERANCANGAN APLIKASI KOPERASI SIMPAN PINJAM BERBASIS WEB (STUDI KASUS KOPERASI MITRA SETIA). Sukabumi: Jurnal Ilmu Ekonomi.
[13] Apache Web Server Complete Guide, Dedoimedo www.dedoimedo.com.
[14] Y. Kustiyahningsih, D. R. (2011). Pemrograman Basis Data Berbasis WEB Menggunakan PHP dan Mysql. Yogyakarta: Graha Ilmu.
[15] Ruli Erinton, R. M. (2017). ANALISIS PERFORMASI FRAMEWORK CODEIGNITER DAN LARAVEL MENGGUNAKAN WEB SERVER APACHE. Bandung: e-Proceeding of Engineering

.