

## SISTEM KEAMANAN JARINGAN DALAM UJIAN ONLINE SMK IPIEMSSURABAYA MENGUNAKAN METODE ADVANCED ENCRYPTION STANDARD (AES)

Jenny Arista (jennyaristaa@gmail.com)<sup>1</sup>, Muhlis Tahir (muhlis.tahir@trunojoyo.ac.id)<sup>2</sup>, Moch.Naufal Haikari (kazamakenkun@gmail.com)<sup>3</sup>, Muhammad Aldito Primatama (alditoprima2014@gmail.com)<sup>4</sup>, Hosniyah (hosniyah793@gmail.com)<sup>5</sup>, Sigit Perdana (sigitsaja41@gmail.com)<sup>6</sup>.

**ABSTRAK:** Di zaman modern ini, di mana Industri 4.0 telah menjadi bagian dari perkembangan zaman, penggunaan teknologi semakin berkembang dengan cepat di berbagai sektor, termasuk kesehatan, militer, dan pendidikan. Dalam bidang pendidikan, ujian online telah menjadi salah satu media pembelajaran yang populer. Namun, meskipun ujian online ini praktis, masih ada celah keamanan yang perlu diperhatikan. Dari celah tersebut maka diperlukan sistem ujian online yang memiliki fitur keamanan yang efektif dan akurat. Salah satu cara untuk mengatasi celah keamanan ini adalah dengan menggunakan salah satu metode enkripsi yang saat ini banyak digunakan, yaitu Advanced Encryption Standard (AES). Berdasarkan hasil penelitian tersebut, terungkap bahwa penggunaan metode enkripsi AES bisa digunakan untuk mengamankan data-data penting dalam ujian online, seperti kata sandi, pertanyaan, dan jawaban. Proses enkripsi dilakukan dengan mengubah teks biasa menjadi nilai hash menggunakan kunci pribadi (private key), sehingga menghasilkan teks bersandi (ciphertext).

**Kata kunci:** Sistem Keamanan Jaringan, Ujian Online, Advanced Encryption Standard.

**ABSTRACT:** In this modern era, where Industry 4.0 has become part of the times, the use of technology is growing rapidly in various sectors, including health, military and education. In the field of education, online exams have become one of the popular learning media. However, while these online exams are practical, there are still security holes that need attention. From this gap, an online examination system is needed that has effective and accurate security features. One way to overcome this security hole is to use one of the currently widely used encryption methods, namely Advanced Encryption Standard (AES). Based on the results of this study, it was revealed that the use of the AES encryption method could be used to secure important data in online exams, such as passwords, questions and answers. The encryption process is performed by converting plain text into a hash value using a private key, resulting in ciphertext.

**Keywords:** Network Security System, Online Exam, Advanced Encryption Standard.

### PENDAHULUAN

Di era modernisasi, teknologi telah semakin berkembang dan digunakan dalam hampir setiap aktivitas manusia. Manfaat komputer tidak lagi hanya sebagai media penghitung, melainkan juga sebagai perangkat dan solusi untuk memecahkan berbagai masalah manusia, terutama sejak masuknya era industri 4.0. Dalam dunia pendidikan, teknologi digunakan sebagai alat bantu sebagai pengembangan, penerapan, penilaian sistem, teknik serta alat bantu guna meningkatkan proses pembelajaran peserta didik.

Dalam bidang teknologi Pendidikan, penerapan sistem informasi internal merupakan hal yang umum terjadi, salah satunya adalah ujian online yang telah diterapkan di hampir seluruh sekolah di Indonesia. Ujian online adalah ujian yang dilakukan secara langsung

melalui perangkat keras/hardware seperti komputer, tablet, dan smartphone yang harus terhubung dengan internet. Dengan adanya ujian online, proses belajar dan pelaksanaan ujian dapat berjalan dengan efektif dari mana saja dan dapat dikerjakan kapan saja, yang sangat cocok untuk siswa yang sedang berada di luar sekolah akibat kendala atau keperluan lain. Namun, meskipun ujian online memiliki banyak keuntungan, masih ada kekurangan yang dapat menyebabkan adanya kecurangan saat proses ujian online antar siswa, karena tidak ada dikontrol langsung oleh pendidik. Kekurangan lainnya yaitu adanya pencurian data dalam proses pelaksanaan ujian. Oleh karena itu, diperlukan sistem keamanan yang dapat meminimalkan kecurangan antar siswa dan pencurian data yang mungkin bisa terjadi. Tindakan pencegahan terhadap serangan

pengguna komputer yaitu dengan menggunakan sistem keamanan komputer dan jaringan agar tidak ada pengakses jaringan ilegal yang akan masuk ke jaringan komputer. Oleh karena itu untuk memastikan keamanan data yang rentan terhadap oknum yang tidak bertanggung jawab, perlu diterapkan sistem keamanan pada komputer dengan metode enkripsi yang sedang populer digunakan, yaitu Advanced Encryption Standard (AES)(Murdowo, 2014).

**METODA**

Dalam tahap metodologi, akan dijelaskan langkah-langkah yang diambil dalam proses penelitian, pengembangan konsep, dan penyelesaian masalah. Selain itu, setiap persamaan matematika yang digunakan dalam metodologi akan diberi nomor secara berurutan dimulai dari angka (1) hingga akhir. Nomor persamaan harus diletakkan di dalam tanda kurung buka dan tutup, dan diletakkan rata kanan. Selain itu, pastikan juga untuk menambahkan satu baris kosong di atas dan di bawah persamaan untuk memudahkan pembacaan.

$$P = \frac{E}{JC(T=const) \cdot \left( P \cdot \left( \frac{E}{E} \right) + (1-P) \right)}$$

**HASIL DAN PEMBAHASAN**

Pada tahap hasil dan pembahasan, aplikasi ujian online telah diujikan dan diimplementasikan pada sebuah institusi pendidikan, yakni SMK IPIEMS Surabaya. Istitusi tersebut telah mengambil peran sebagai subjek penelitian, dimana aplikasi ujian online telah diujikan dalam kondisi yang sebenarnya.

**1. Tahap Analisis**

Ketika merancang aplikasi untuk media ujian online dengan menerapkan metode AES, ada beberapa komponen penting yang perlu diperhatikan. Perancangan aplikasi harus mempertimbangkan faktor-faktor seperti penggunaan teknologi enkripsi yang tepat, keamanan data, interaksi pengguna yang muda, serta ketersediaan jaringan internet yang memadai untuk memastikan kinerja aplikasi yang optimal.

- a. Apache HTTP Server merupakan software yang mendukung multitasking dan menyediakan layanan untuk software lain yang terhubung kepadanya, contohnya web browser. Apache awalnya ditemukan untuk

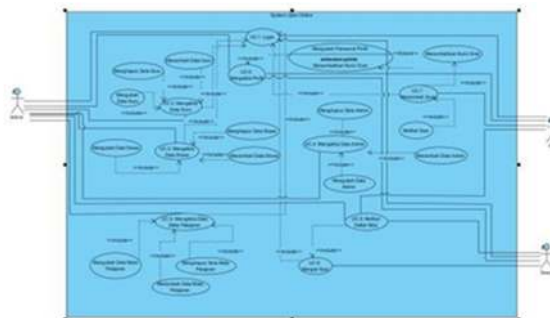
digunakan dalam sistem operasi Linux/Unix, namun seiring berjalannya waktu dikembangkan lagi untuk bekerja dengan sistem operasi lainnya.

- b. Penerapan sistem keamanan jaringan dalam proses pengamanan data ujian online di SMK IPIEMS sangat krusial. Dalam konteks ini, salah satu media yang digunakan adalah database MySQL, yang memiliki kemampuan untuk menampung satu atau beberapa tabel data. MySQL digunakan sebagai database untuk menyimpan data ujian online yang dienkripsi menggunakan metode AES sehingga data tersebut dapat diakses secara aman dan hanya dapat diakses oleh pihak yang berwenang(Sugiyono, 2019)
- c. Dalam pembuatan aplikasi ujian online, digunakan sebuah framework yang bernama CodeIgniter. CodeIgniter adalah sebuah kerangka kerja aplikasi web yang berfungsi untuk membangun aplikasi PHP dinamis dengan menerapkan konsep Model View Controller (MVC) development pattern. CodeIgniter menyediakan berbagai library yang dapat memudahkan proses pengembangan aplikasi, sehingga mempercepat proses pembuatan aplikasi ujian online (Erinton et al., 2017).

**2. Desain**

Proses desain sistem dilakukan dengan menggunakan Unified Modeling Language (UML) yang melibatkan penggunaan beberapa diagram, termasuk Use Case Diagram dan Activity Diagram. Use Case Diagram digunakan untuk menggambarkan interaksi antara pengguna dan sistem yang menjalankan tugas tertentu. Sementara itu, Activity Diagram berfungsi untuk menggambarkan urutan aktivitas dan tindakan yang terjadi dalam proses sistem.

- a. Use Case



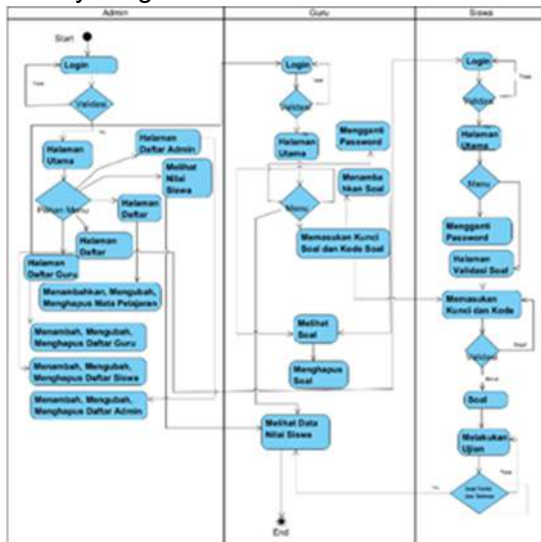
Gambar 1 Use Case

keamanan data dan mencegah orang yang tidak berenang untuk mengakses atau membaca data ujian online. Dalam implementasi sistem ujian online, penerapan metode AES sangat penting untuk memastikan keamanan dan keandalan suatu sistem.

### 1. Tampilan Aplikasi

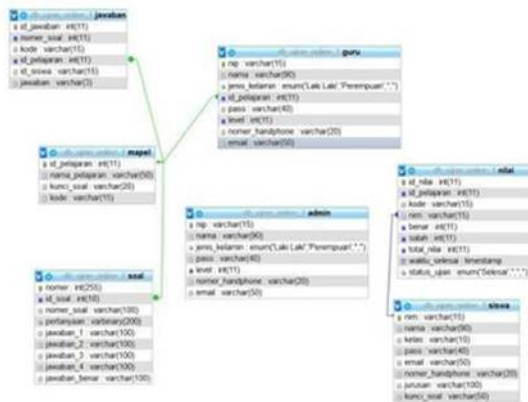
Berikut ini adalah tampilan antarmuka web ujian online yang telah berhasil dikembangkan oleh peneliti. Antarmuka web ini telah diselesaikan dan siap digunakan oleh pengguna.

#### b. Activity Diagram

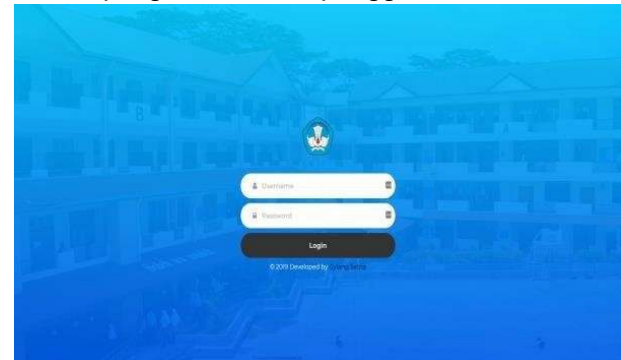


Gambar 2 Aktifitas Diagram

#### c. Desain Basis Data



Gambar 3 Basis Data



Gambar 4 Halaman Login

Setelah memasukkan alamat untuk mengakses aplikasi ujian online, pengguna (guru, siswa, dan admin) akan diarahkan ke halaman login. Halaman login ini merupakan tempat untuk memasukkan informasi akun yang telah terdaftar sebelumnya. Setelah masuk ke dalam akun, pengguna akan diarahkan ke halaman akses yang sesuai dengan hak akses masing-masing.



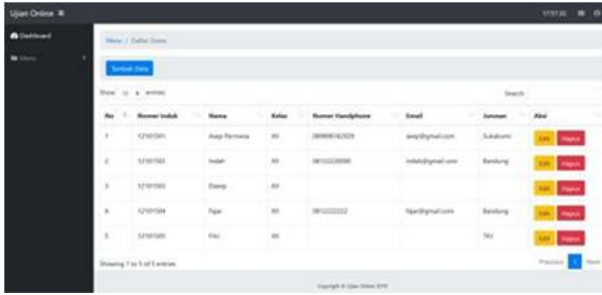
Gambar 5 Dashboard Admin.

### HASIL DAN PEMBAHASAN

Algoritma AES diterapkan pada komponen-komponen penting dari sistem ujian online, seperti kata kunci akun, pertanyaan, dan jawaban untuk menjaga keamanan data tersebut. Dalam rangka menjaga keamanan, data tersebut dienkripsi dengan menggunakan metode AES sehingga teks asli akan berubah menjadi teks acak yang tersimpan didalam database MYSQL (Yudha & Laluma, 2019). Proses pengacakan ini bertujuan untuk memastikan

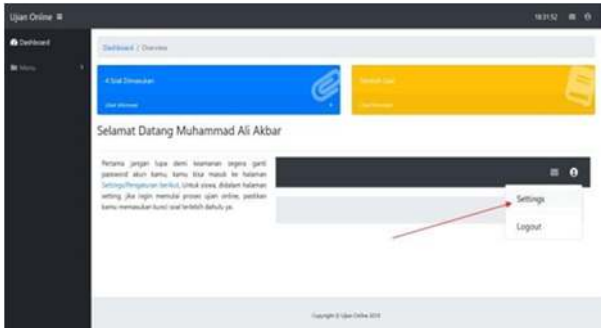
Halaman ini menyajikan beberapa menu yang terkait dengan manajemen akun pengguna yang memiliki akses ke aplikasi ujian online. Pengguna dapat melakukan beberapa tindakan, seperti menambahkan, mengedit, atau menghapus akun pengguna serta data mata pelajaran. Selain itu, bagi pengguna dengan hak akses sebagai admin, juga dapat melihat daftar nilai semua siswa dan mata pelajaran tanpa dapat merubahnya. Dengan demikian, halaman ini memudahkan pengguna untuk melakukan manajemen akun dan data

terkait dalam aplikasi ujian online secara efektif dan efisien.

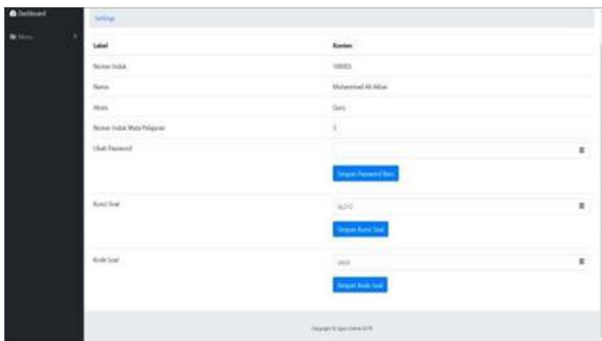


Gambar 6 Pengelola Siswa

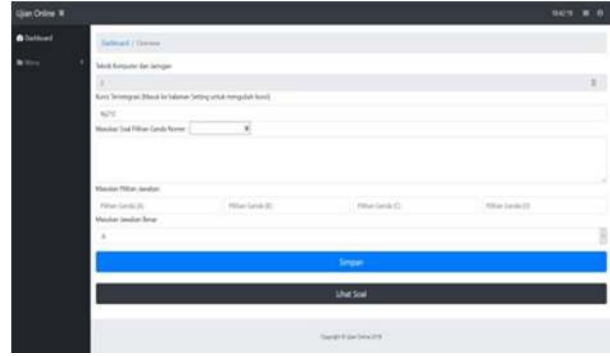
Berikutnya, untuk mengakses fitur-fitur yang khusus disediakan bagi guru, tersedia sebuah dashboard yang menyerupai halaman akses admin. Akan tetapi, terdapat beberapa perbedaan menu akses yang disediakan khusus untuk guru, seperti menu untuk menambah, menghapus, dan mengubah soal ujian, serta akses khusus untuk menambahkan atau mengubah kunci soal pada halaman profil. Kunci ini memiliki fungsi penting dalam proses enkripsi dan dekripsi pada soal dan jawaban dalam aplikasi ujian online. Dengan demikian, guru dapat memaksimalkan penggunaan fitur-fitur pada aplikasi ujian online dan meningkatkan kinerja dalam mengelola soal dan kunci soal.



Gambar 7 Dashboard Guru

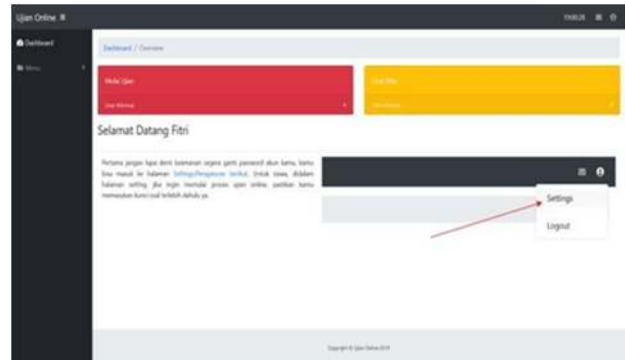


Gambar 8 Profile Guru

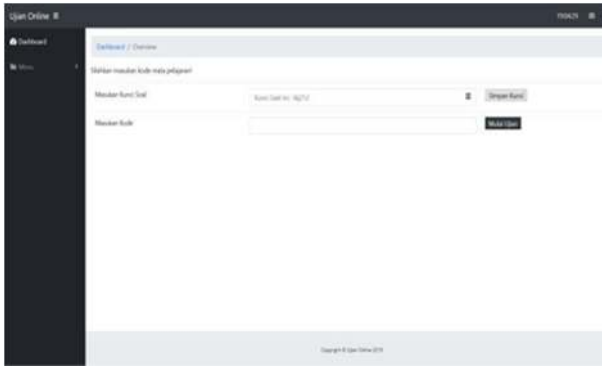


Gambar 9 Membuat Soal

Setelah itu, saat siswa mengakses halaman ujian online, mereka akan diberikan akses untuk mengisi soal ujian. Sebelum memulai mengerjakan soal, siswa akan diminta untuk memasukkan kunci soal yang telah dibuat sebelumnya oleh guru. Kunci soal ini bertujuan untuk memastikan bahwa siswa memiliki akses yang sah ke dalam ujian dan menghindari adanya kecurangan dalam proses pengisian jawaban. Jika siswa gagal memasukkan kunci soal yang tepat, mereka tidak dapat mengisi soal dan halaman akan menampilkan pesan kesalahan. Namun, jika kunci soal benar, siswa dapat dengan mudah mengisi dan menyelesaikan soal ujian dengan menggunakan antarmuka yang intuitif dan mudah digunakan. Hal ini dilakukan untuk memastikan bahwa siswa hanya dapat mengakses soal yang telah diizinkan oleh guru dan meningkatkan keamanan sistem ujian online. Selain itu, dengan memasukkan kunci soal, siswa juga akan memperoleh akses untuk menjawab soal dan melanjutkan proses pengisian jawaban dengan lebih mudah dan terstruktur.



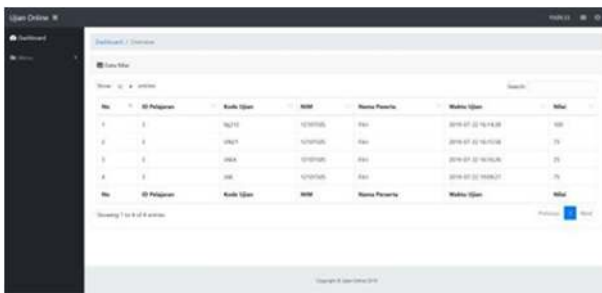
Gambar 10 Dashboard Siswa



Gambar 11 Validasi Soal



Gambar 12 Pengisian Soal



Gambar 13 Daftar Nilai

Halaman daftar nilai pada aplikasi ujian online memberikan akses kepada semua pengguna untuk melihat nilai siswa. Namun, hak akses yang dimiliki berbeda-beda tergantung pada peran pengguna. Admin dapat melihat nilai siswa dari semua mata pelajaran, sementara guru hanya dapat melihat nilai siswa dari mata pelajaran yang diajar. Siswa hanya dapat melihat daftar nilai sesuai dengan akun yang dimilikinya. Dengan adanya fitur ini, setiap pengguna dapat dengan mudah memantau progres belajar dan mengevaluasi performa siswa dengan lebih efektif.

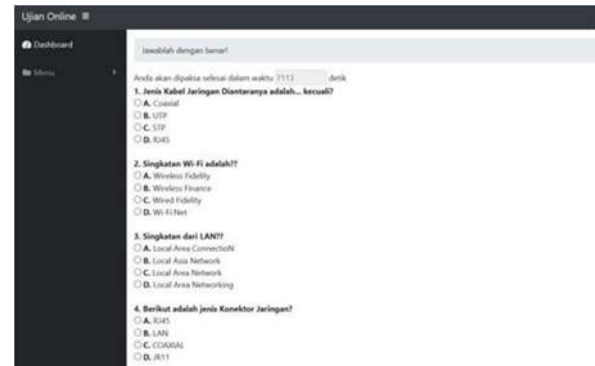
## 2. Pengujian Keamanan

Dalam melakukan pengujian, dilakukan pengecekan terhadap kebenaran pengisian kunci soal. Jika siswa salah memasukkan kunci soal

pada halaman validasi, maka siswa tidak dapat mengisi soal. Sebaliknya, jika siswa memasukkan kunci soal dengan benar, maka halaman soal akan muncul dan siswa dapat mengisi soal dengan normal. Pengujian juga dilakukan untuk mengecek apakah pengguna dengan hak akses sebagai guru dan admin dapat menambah, mengubah, dan menghapus soal dengan baik. Hasil pengujian menunjukkan bahwa sistem dapat berfungsi dengan baik dan berhasil mencegah pengguna tidak sah untuk mengakses dan mengubah soal ujian.

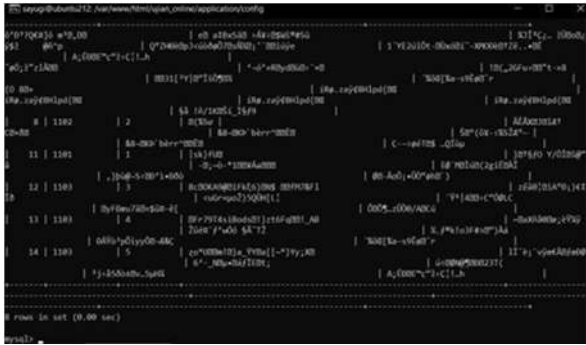


Gambar 14 Soal (Salah)



Gambar 15 Soal (Benar)

Berikut ini adalah uji coba dengan skenario ketika ada pihak yang tidak memiliki hak akses berhasil masuk ke dalam database dan mencoba mencuri kunci jawaban. Tujuan dari pengujian ini adalah untuk mengevaluasi keamanan sistem dan memastikan bahwa sistem keamanan jaringan dapat mencegah akses yang tidak sah ke database dan melindungi kunci jawaban dari pencurian. Dalam pengujian ini, akan disimulasikan serangan dari luar dengan mencoba mengakses database dan mencari cara untuk mendapatkan kunci jawaban yang dilindungi oleh sistem keamanan jaringan. Hasil dari pengujian ini akan membantu peneliti untuk meningkatkan sistem keamanan jaringan dan memastikan bahwa data pengguna terlindungi dari serangan luar yang tidak diinginkan.



Gambar 16 Skenario Pengujian Pencurian Kunci Jawaban.

## KESIMPULAN DAN SARAN

Berdasarkan desain sistem dan pengujian yang telah dilakukan, penelitian ini menemukan beberapa hal tentang Sistem Keamanan Jaringan Dalam Ujian Online SMK IPIEMS Surabaya Menggunakan Metode Algoritma Advanced Encryption Standard (AES).

1. Sistem keamanan jaringan pada aplikasi ujian online dapat memberikan keamanan pada soal dan jawaban yang tersimpan dalam database, sehingga tidak dapat diakses oleh pihak yang tidak berwenang.
2. Dengan penerapan ujian online, biaya ujian dapat dikurangi secara signifikan dibandingkan dengan metode konvensional.

## DAFTAR PUSTAKA

### Jurnal

- Erinton, R., Negara, R. M., & Sanjoyo, D. D. (2017). Analisis Performasi Framework Codeigniter dan Laravel Menggunakan Web Server Apache. *Core*, 3565–3572.
- Murdowo, S. (2014). Mengenal Perhitungan Enkripsi Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Infokam*, 32–40.
- Sugiyono. (2019). Pengembangan Media Simulator Pada Pendidikan Dan Pelatihan Foam Tender Operation And Defensive Driving di Balai Pendidikan dan Pelatihan Penerbangan Palembang. *Program Pascasarjana Universitas Pgri Palembang*, 108–119.
- Yudha, G. S., & Laluma, R. H. (2019). *Sistem Keamanan Jaringan Dalam Ujian Online Sma/Smk Menggunakan Metode Algoritma Advanced Encryption Standard (AES)*. 4(2).