Implementasi Kriptografi AES pada Sistem Akses Konten Digital untuk Karya Hasil Anggota Unit Pochu Genshiken ITB

1st Muhammad Raihan Aulia, 2nd Dr. Ir. Rinaldi, M.T.
[12]*School of Electrical Engineering and Informatics*
Institut Teknologi Bandung
Bandung, Indonesia
[1]18220031@std.stei.itb.ac.id
[2]rinaldi@informatika.org

***Abstrak*— Pochu Genshiken ITB adalah sebuah organisasi yang bergerak pada bidang kekaryaan. Dalam kegiatannya, Genshiken menghasilkan karya dalam konten digital karena kemudahan dalam penyebaran dan pembuatan konten digital. Karena kemudahan tersebut, terdapat kekhawatiran terjadinya duplikasi dan penyebaran ilegal konten tanpa sepengetahuan pembuat konten. Untuk mengatasi permasalahan tersebut, diterapkan konsep enkripsi dengan menggunakan AES dan pembatasan akses untuk mengimplementasikan sistem akses konten digital sehingga mencegah pencurian dan penyebaran konten digital tanpa hak. Sistem terdiri dari *back-end* berbasis *server*, aplikasi Android pengguna untuk mengakses konten, dan aplikasi web admin untuk mengelola konten. Hasil pengujian fungsional dan *user assessment test* menunjukkan sistem berfungsi dengan baik dalam memenuhi spesifikasi yang harus dipenuhi oleh sistem dan kebutuhan pengguna, serta melindungi konten digital dari pencurian dan duplikasi tanpa izin.**

***Kata kunci*— kriptografi, sistem akses konten digital, konten digital, AES, Pochu Genshiken ITB**

I. PENDAHULUAN

Perkembangan teknologi digital telah membawa banyak perubahan dalam berbagai aspek kehidupan. Salah satu aspek tersebut adalah aspek karya seni yang menghasilkan karya-karya dalam bentuk konten digital [1]. Kemudahan dalam pembuatan dan penyebaran konten digital mengakibatkan konten digital semakin populer di kalangan penggemar seni. Namun, dengan kemudahan yang ditawarkan oleh konten digital, timbul berbagai masalah terkait hak cipta konten digital seperti duplikasi dan penyebaran tanpa diketahui pembuat konten [2].

Unit Pochu Genshiken ITB merupakan unit kegiatan mahasiswa yang bergerak dalam bidang kekaryaan. Karya-karya tersebut merupakan ekspresi kreatif anggota Unit Pochu Genshiken ITB [3]. Konten digital yang dihasilkan berjenis audio, teks, gambar, dan video. Karena penggunaan konten digital dalam mengekspresikan jiwa kekaryaan, Genshiken ITB tidak lepas dari permasalahan konten digital yang mengancam hak cipta pembuat konten atas konten digital yang dibuatnya. Dengan adanya ancaman tersebut, konten digital yang sudah dibuat oleh anggota unit Pochu Genshiken ITB tidak dapat disebarluaskan tanpa mengancam hak cipta yang dimiliki oleh pembuat konten.

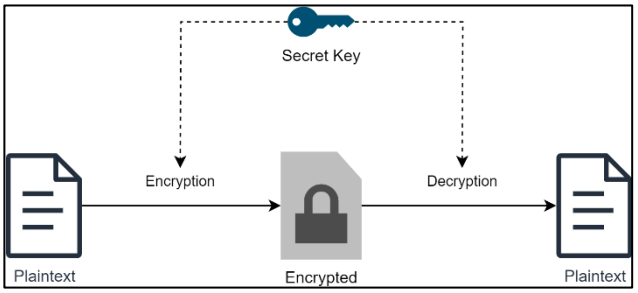
Didasari permasalahan yang sudah disebutkan sebelumnya, penelitian ini bertujuan untuk mengembangkan dan mengevaluasi kinerja sistem akses konten digital yang menerapkan enkripsi dan pembatasan akses untuk melindungi konten digital di lingkungan Unit Pochu Genshiken ITB. Sistem ini diharapkan dapat meningkatkan keamanan dan penyebaran konten digital hasil anggota Pochu Genshiken ITB.

II. LANDASAN TEORI

Berikut beberapa contoh penelitian yang terkait dengan pengembangan sistem akses konten.

A. Kriptografi Kunci-simetris

Kriptografi kunci-simetris adalah metode enkripsi yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi pesan [4]. Penggunaan algoritma kunci-simetris dalam distribusi konten digital memungkinkan konten dienkripsi dan hanya bisa digunakan menggunakan kunci tersebut. Kriptografi kunci-simetris dapat diilustrasikan sesuai dengan gambar 1.

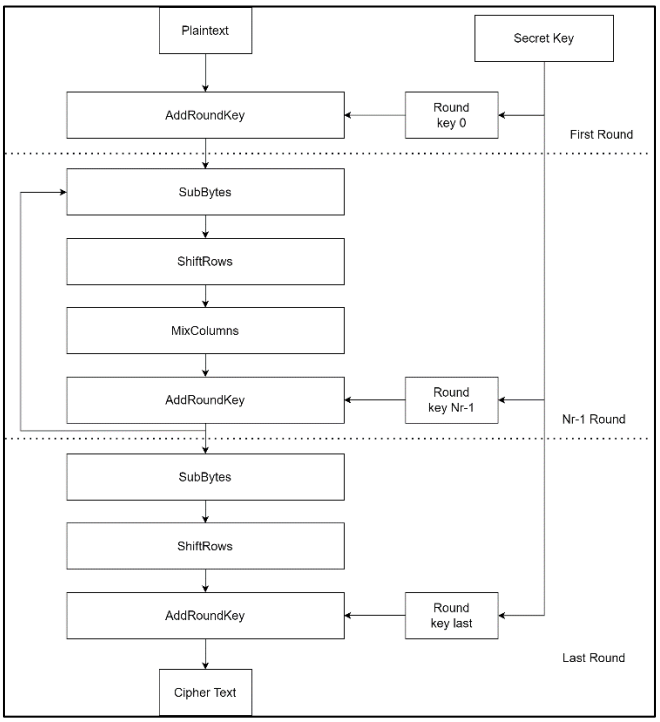


Gambar 1 Ilustrasi Kriptografi Kunci-simetris

B. Advanced Encryption Standard (AES)

AES adalah sebuah standar enkripsi yang sudah digunakan pada banyak tempat. Algoritma AES, yaitu Rijndael yang sudah dimodifikasi, ditetapkan sebagai standar enkripsi kriptografi kunci simetris yang menggantikan DES. Pergantian ini dikarenakan kelemahan DES yang sudah cukup mudah dieksploitasi sehingga tidak lagi aman [5]. Terdapat tiga panjang kunci yang dapat digunakan pada AES yaitu 128 bit, 192 bit, dan 256 bit. Dalam proses enkripsi, terdapat beberapa putaran dengan jumlah yang sesuai dengan panjang kunci yang digunakan yaitu 10 putaran, 12 putaran, dan 14 putaran. Kedua hal ini yang mengakibatkan AES memiliki tingkat keamanan yang lebih tinggi dibandingkan DES.

Secara ringkas, mekanisme *block cipher* pada AES dilakukan dengan pembuatan *round key* dari sebuah kunci rahasia yang sudah ditentukan sebelumnya. Setelah *round key* ditentukan, dilakukan substitusi bit-bit pada data blok dengan menggunakan *lookup table* yang sudah didefinisikan. Setelah itu, dilakukan perubahan posisi bit pada satu byte dan diikuti dengan pengubahan posisi bit ke bit lainnya. Proses-proses ini dilakukan sesuai dengan gambar 2.



Gambar 2 Mekanisme Blok Cipher pada AES Secara Ringkas [5]

Secara keseluruhan, AES lebih cepat dibandingkan dengan DES tetapi membutuhkan memori yang lebih besar juga. Hal ini dikarenakan kerja AES yang melakukan enkripsi *plaintext* dengan ukuran yang lebih besar, yaitu 128 bit, sedangkan DES hanya sebesar 64 bit [6].

C. Penelitian Terkait

1. *Research and implementation of digital rights management model for vector graphics [7]*

Penelitian ini mengimplementasikan *digital rights management* (DRM) untuk melindungi konten digital berupa gambar vektor. Teknologi yang digunakan pada sistem pada penelitian ini adalah teknologi enkripsi dan *watermark*. Penelitian ini membuktikan penggunaan enkripsi yang dapat digunakan sebagai perlindungan pembajakan pada konten digital berjenis gambar vektor.

2. *Selective Encryption of the Audio Extracted from the Video Streamed Over the Content Delivery Network [8]*

Penelitian ini melakukan teknik pemisahan aspek audio dari konten digital berjenis video dan aspek audio dienkripsi menggunakan algoritma kriptografi kunci-simetris. Penelitian ini memberikan informasi mengenai sebuah cara untuk mengamankan konten digital pada jaringan *internet* yang tidak aman sehingga sampai kepada pengguna konten digital yang berhak menggunakan konten tersebut.

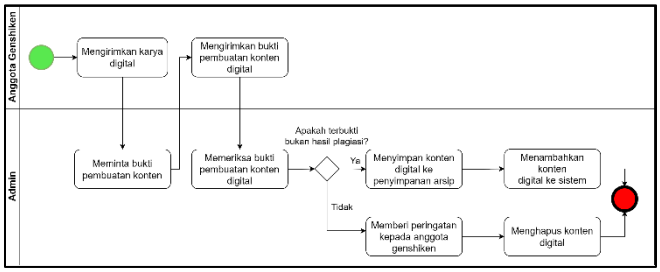
III. RANCANGAN SOLUSI

Sistem akses konten terdiri dari dua komponen utama, yaitu pengelolaan konten digital dan akun pengguna pada sistem serta pengaksesan konten digital yang terdapat pada sistem.

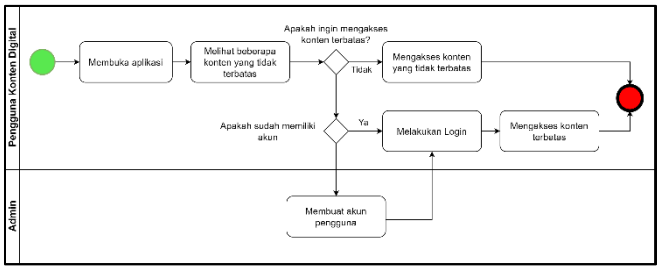
A. Proses Bisnis Sistem Solusi

Dalam pelaksanaan fungsi sistem solusi, terdapat dua proses bisnis yang berbeda, yaitu proses bisnis penambahan konten digital dan pengaksesan konten digital oleh pengguna konten.

Proses bisnis terkait penambahan konten digital dimulai ketika anggota Genshiken mengirimkan karya digital miliknya untuk ditambahkan pada sistem. Admin akan meminta bukti pembuatan konten kepada anggota tersebut dan akan dibalas dengan bukti pembuatan konten digital. Jika bukti yang dikirimkan sesuai dan cukup membuktikan, konten akan ditambahkan pada sistem dan konten juga disimpan pada arsip organisasi. Jika bukti pembuatan tidak cukup, konten digital akan dibuang dan anggota tersebut akan diberi peringatan. Proses bisnis terkait penambahan konten digital dapat diilustrasikan sesuai dengan gambar 3.



Gambar 3 Proses Bisnis Sistem Solusi Terkait Penambahan Konten Digital



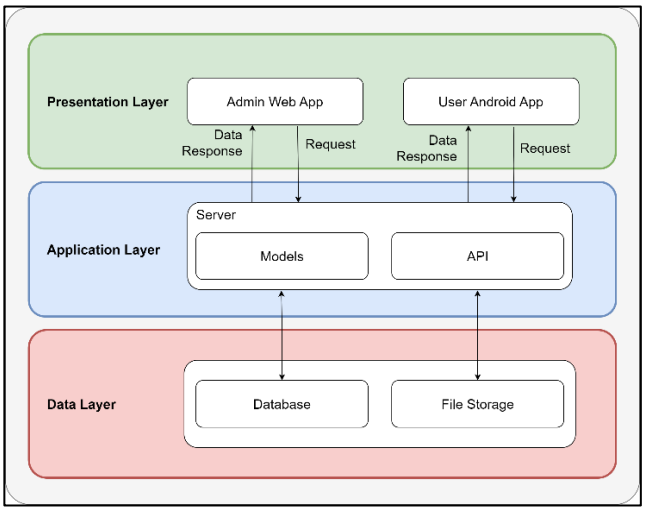
Gambar 4 Proses Bisnis Sistem Solusi Terkait Pengaksesan Konten Digital

Proses bisnis terkait pengaksesan konten digital dimulai ketika pengguna konten membuka aplikasi akses konten dan melihat konten yang tidak terbatas. Jika pengguna ingin mengakses konten digital tanpa batasan akses, pengguna dapat langsung memilih dan mengakses konten tersebut. Jika pengguna ingin menggunakan konten digital dengan akses terbatas, pengguna harus terlebih dahulu melakukan *login* dengan akun yang disediakan oleh admin dan memilih konten digital terbatas yang diinginkan. Proses bisnis pengaksesan konten dapat diilustrasikan sesuai dengan gambar 4.

B. Arsitektur Sistem

Arsitektur sistem secara keseluruhan terbagi atas tiga *layer*, yaitu *presentation layer*, *application layer*, dan *data layer*. Pada *data layer*, terdapat sebuah basis data untuk menyimpan data dan sebuah *file storage* untuk menyimpan konten digital sistem. *application layer* terdiri atas sebuah server yang memiliki API untuk menghubungkan server yang bekerja sebagai *controller* dan *Models* yang menghubungkan server dengan *database* dengan aman. Pada lapisan ini juga dilakukan enkripsi konten digital sebelum konten disimpan pada *file storage*. *Application layer* dan *data layer* berkomunikasi secara langsung.

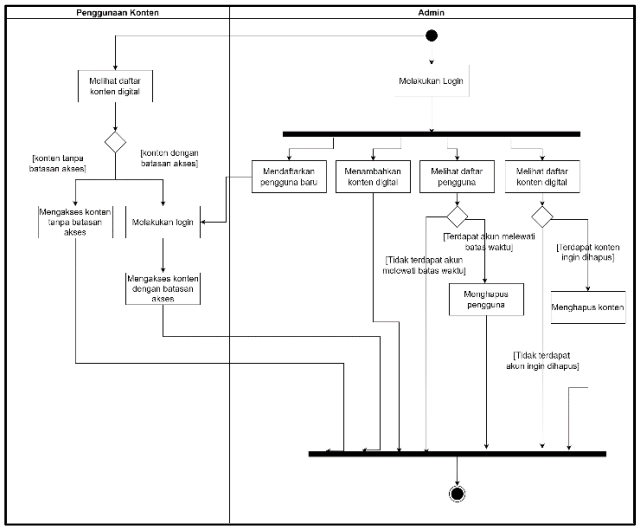
Presentation layer terdiri atas aplikasi *web* untuk admin dan aplikasi android yang berhubungan langsung dengan pengguna. Lapisan ini berguna untuk menghubungkan pengguna dengan sistem. Untuk menghubungkan *presentation layer* dengan *application layer*, digunakan protokol HTTPS untuk mengamankan data yang dikirimkan antara *presentation layer* dan *application layer*.



Gambar 5 Arsitektur Sistem

C. *Diagram Aktivitas Sistem*

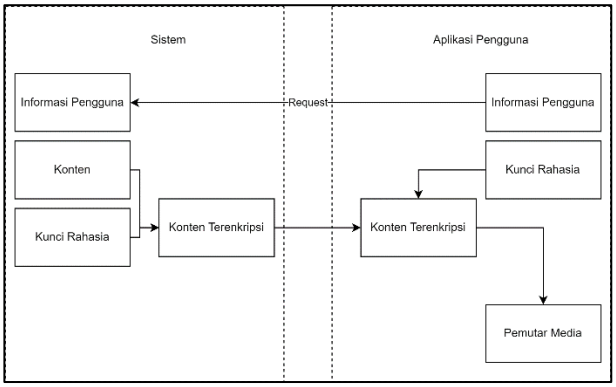
Penggunaan sistem untuk pengguna admin dimulai dari melakukan *login*. Dengan melakukan *login*, pengguna dapat melakukan fitur-fitur admin yang diperlukan untuk mengelola akun dan mengelola konten digital pada sistem. Untuk pengguna konten, aktivitas sistem dimulai dengan melihat daftar konten digital. Jika pengguna ingin mengakses konten digital tanpa batasan akses, pengguna dapat langsung mengakses konten tersebut. Jika pengguna ingin mengakses konten dengan batasan akses, pengguna harus melakukan *login* terlebih dahulu dengan menggunakan akun yang sudah disediakan oleh admin sebelum mengakses konten tersebut.



Gambar 6 Alir Aktivitas Sistem

D. *Skema Sistem Akses Konten*

Pada sistem, konten dienkripsi menggunakan sebuah kunci rahasia yang sudah ditentukan. Ketika aplikasi pengguna melakukan *request* konten, *back-end* sistem akan memberikan konten terenkripsi kepada pengguna. Pada aplikasi pengguna, dilakukan dekripsi menggunakan kunci yang sama dan konten hasil dekripsi diputar menggunakan pemutar media pada aplikasi pengguna.



Gambar 7 Skema Sistem Akses Konten

IV. IMPLEMENTASI

Sistem yang dikembangkan berdasarkan rancangan solusi adalah sistem akses konten yang terdiri dari aplikasi Android pengguna konten untuk mengakses konten dan aplikasi *web* admin sekaligus *back-end* sistem untuk mengelola konten digital dan akun pengguna. Lingkungan pengembangan perangkat lunak sebagai berikut.

1. Pengembangan aplikasi *web* admin menggunakan Visual Studio Code sebagai *code editor*, bahasa pemrograman Python, HTML, CSS, dan JavaScript, SQlite sebagai database, dan *web framework* Flask yang didukung dengan Gunicorn.
2. Pengembangan aplikasi android pengguna menggunakan Android Studio, bahasa pemrograman Kotlin, dan didukung dengan native library Android dan library pihak ketiga.dmin menggunakan Visual Studio Code sebagai code editor, bahasa pemrograman Python, dan beberapa library yang mendukung fungsional aplikasi.

A. *Implementasi Basis Data*

Basis data sistem diimplementasikan sebagai dua buah tabel, yaitu tabel user dan tabel media. Tabel user memiliki empat buah atribut dengan penjelasan sebagai berikut.

1. **username**, menyimpan nilai *username* dan digunakan sebagai identifier unik. Atribut ini bertipe *text.*
2. **password,** menyimpan hasil hash password pengguna. Atribut ini bertipe *text.*
3. **role,** menyimpan peran pengguna pada sistem. Bernilai “admin” atau “user”. Atribut ini bertipe *text.*
4. **date_created,** menyimpan tanggal akun dibuat. Atribut ini bertipe *text.*

Tabel media digunakan untuk menyimpan data-data yang berkaitan dengan konten digital yang terdapat pada sistem.

Tabel media memiliki tujuh buah atribut dengan penjelasan sebagai berikut:

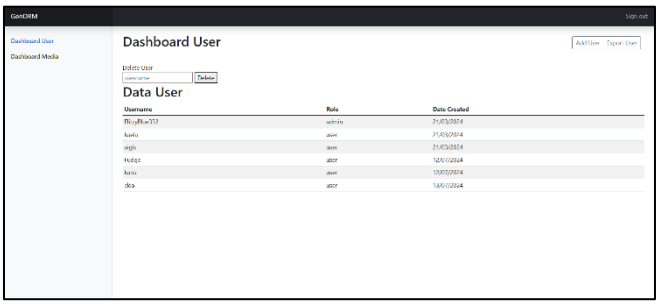
1. **id**, sebagai *identifier record* konten digital. Atribut ini bertipe *integer*.
2. **title,** menyimpan data judul konten digital. Atribut ini bertipe *text.*
3. **type,** menyimpan tipe konten digital. Bernilai "video", "audio", atau "image". Atribut ini bertipe *text.*
4. **fname,** menyimpan nama *file* konten digital pada sistem. Atribut ini bertipe *text.*
5. **artist**, nama pembuat konten digital.
6. **date_created,** menyimpan tanggal konten digital ditambahkan pada sistem. Atribut ini bertipe *text.*
7. **auth,** menyimpan nilai batasan konten digital. Atribut ini bertipe *boolean.*

B. Implementasi Antarmuka Aplikasi Web Admin

Antarmuka aplikasi *web* admin terdiri atas lima halaman, yaitu halaman *login*, halaman *dashboard user*, halaman *dashboard media*, halaman *add user*, dan halaman *add media*. Ketika pengguna belum mendapatkan akses pada sistem dan mencoba membukan aplikasi *web* pengguna, Halaman *login* akan terbuka dan meminta pengguna untuk melakukan *login* terlebih dahulu. Pengguna dapat melakukan *login* dengan menggunakan akun yang sudah ada dan menekan tombol "Sign in".

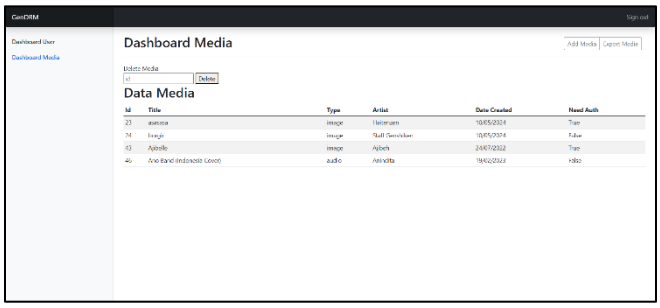
Gambar 8 Halaman Login

Halaman *dashboard user* akan ditampilkan ketika pengguna menekan *menu item dashboard user* atau pengguna baru saja melakukan *login*. Halaman ini berisi data akun pengguna yang terdapat pada sistem. Pada halaman ini, terdapat dua tombol, yaitu tombol "export user" untuk melakukan *export* seluruh data pengguna dan tombol "add user" untuk pindah ke halaman *add user*.



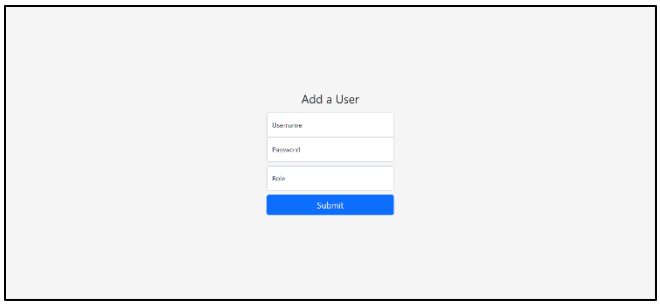
Gambar 9 Halaman Dashboard User

Halaman *dashboard media* akan ditampilkan ketika pengguna menekan *menu item dashboard user*. Halaman ini berisi data konten digital yang terdapat pada sistem. Pada halaman ini, terdapat dua tombol, yaitu tombol "export media" untuk melakukan *export* seluruh data konten digital dan tombol "add media" untuk pindah ke halaman *add media*.



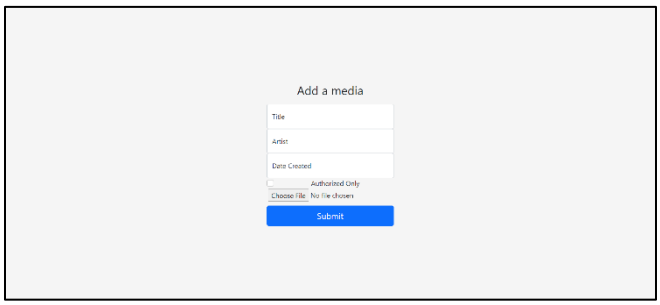
Gambar 10 Halaman Dashboard Media

Halaman *add user* akan ditampilkan ketika pengguna menekan tombol "add user" pada *dashboard user*. Halaman ini berisi *entry field username*, *password*, dan *role* dari akun pengguna yang akan ditambahkan. Ketika tombol "Submit" ditekan, akun pengguna akan ditambahkan.



Gambar 11 Halaman Add User

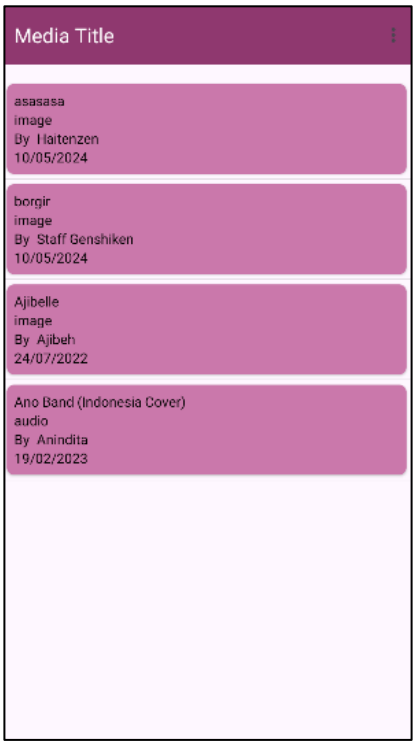
Halaman *add media* akan ditampilkan ketika pengguna menekan tombol "add media" pada *dashboard media*. Halaman ini berisi *entry field title*, *artist*, dan *date created.* Terdapat juga *checkbox auth* dan *entry file* konten dari konten digital yang akan ditambahkan. Ketika tombol "Submit" ditekan, konten digital akan ditambahkan.



Gambar 12 Halaman Login Admin

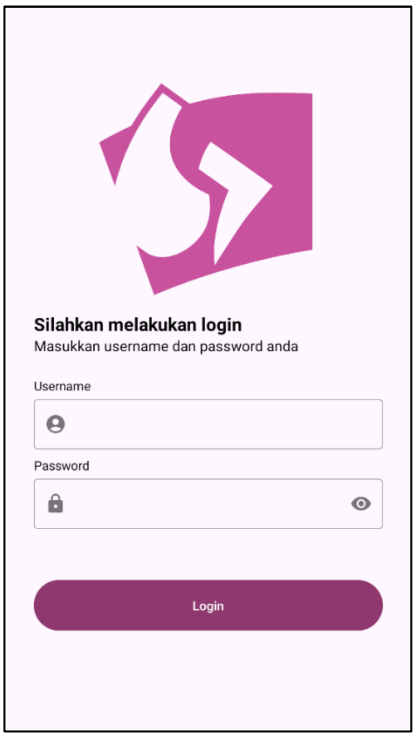
C. *Implementasi Antarmuka Aplikasi Android Pengguna Konten*

Antarmuka aplikasi Android pengguna konten terdiri atas dua halaman, yaitu halaman *login* dan halaman daftar konten digital. Ketika pengguna belum melakukan *login* dan membuka aplikasi, halaman daftar konten digital yang hanya berisi konten digital tanpa batasan akses akan ditampilkan. Jika pengguna sudah melakukan *login*, akan ditampilkan daftar konten yang berisi konten digital tanpa batasan akses dan konten digital dengan batasan akses. Ketika pengguna mengetuk salah satu konten pada daftar, konten digital yang dipilih akan dimainkan.



Gambar 13 Halaman Daftar Konten Digital

Halaman *Login* akan ditampilkan ketika pengguna yang belum melakukan *login* membuka tombol menu dan menekan menu "Login". Pada halaman ini, terdapat *entry field username* dan *password*. Ketika pengguna menekan tombol "Login", perintah *login* akan dijalankan.



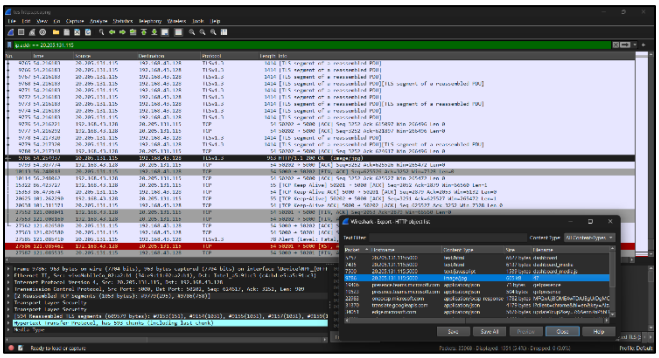
Gambar 14 Halaman Login Aplikasi Pengguna Konten

V. PENGUJIAN

A. *Functional Testing*

Dalam *functional testing* yang dilakukan, dibuat beberapa skenario pengujian dengan ekspektasi keluaran yang diharapkan untuk setiap unit pengujiannya. Jika keluaran yang dihasilkan ketika unit pengujian dilaksanakan sesuai dengan ekspektasi, pengujian dianggap berhasil. Sebaliknya, pengujian dianggap gagal jika keluaran tidak sesuai dengan ekspektasi.

Functional Testing yang dilaksanakan pada sistem dilakukan secara *black box* testing dan *white box* testing. Unit pengujian yang dilakukan dengan cara *black box* testing dilakukan dengan berinteraksi langsung dengan antarmuka pengguna, sementara unit pengujian yang dilaksanakan dengan cara *white box testing* dilaksanakan dengan memanggil API *endpoint* dan menggunakan aplikasi lain untuk melakukan penangkapan paket.



Gambar 15 Tangkapan Layar Penangkapan Paket

Terdapat 26 skenario pada *functional test*. Skenario terdiri dari skenario *positive* untuk pemenuhan fungsionalitas dan

skenario *negative* untuk menguji penanganan *error*. Unit pengujian yang berhasil dinilai dengan "PASS", unit pengujian yang gagal beri nilai "FAIL", dan unit pengujian yang tidak berhasil dijalankan karena alasan teknis diberi nilai "UNEXECUTED".

Tabel 1. Rangkuman Hasil *Functional Testing*

Status	Definisi	Jumlah Unit Pengujian
PASS	Skenario berhasil dijalankan dan keluaran sesuai dengan ekspektasi	26
FAIL	Skenario berhasil dijalankan, tetapi keluaran tidak sesuai dengan ekspektasi	0
UNEXECUTED	Skenario tidak dapat dilakukan karena masalah teknis	0

B. User Acceptance Testing (UAT)

UAT dilakukan dengan 13 penguji yang mewakili pengguna sistem. Pengujian dilakukan dengan penguji melakukan pengunduhan dan pemasangan aplikasi pengguna konten. Skenario dan hasil pengujian sesuai dengan tabel 2.

Tabel 2. Hasil *UAT*

No.	Skenario	Jumlah Penguji Berhasil	Jumlah Pengguna berdasarkan pengalaman penyelesaian				
			Sangat Sulit	Sulit	Sedang	Mudah	Sangat Mudah
1	Melihat daftar konten tanpa batasan akses	13	0	0	0	0	13
2	Mengakses konten digital tanpa batasan akses	13	0	0	0	0	13
3	Melakukan Login	13	0	0	1	2	10
4	Melihat daftar konten lengkap	13	0	0	0		13
5	Mengakses Konten dengan Batasan Akses	13	0	0	0	1	12
6	Mencoba memicu halangan screenshot	13	0	0	0	0	13

Berdasarkan hasil pengujian pada tabel 2, seluruh pengguna dapat menyelesaikan skenario pengujian dan mayoritas penguji menyelesaikan skenario pengujian dengan mudah. Dengan hasil tersebut, dapat diambil kesimpulan sistem yang dikembangkan mudah digunakan oleh pengguna.

VI. KESIMPULAN

Kesimpulan dari penelitian ini adalah rancangan sistem akses konten untuk melindungi konten digital anggota Genshiken ITB dapat meningkatkan keamanan konten digital dan menyediakan cara untuk penyebaran konten digital di luar lingkungan Genshiken ITB. Dengan adanya opsi penyebaran konten digital dan kemudahan penggunaan sistem, penyebaran konten digital hasil anggota Genshiken ITB dapat meningkat. Hasil pengujian fungsional dan *user acceptance test* dengan skenario-skenario yang sudah dibuat sebelumnya menunjukkan sistem telah berfungsi dengan baik sesuai dengan spesifikasi yang sudah ditentukan.

Penggunaan algoritma AES pada sistem akses konten untuk melakukan enkripsi konten digital dapat meningkatkan keamanan konten digital. Dengan menggunakan metode ini, konten digital hanya dapat diakses oleh pengguna yang memiliki kunci, yaitu pengguna yang menggunakan aplikasi pengguna konten, dan pengguna konten yang tidak memiliki kunci yang sesuai tidak dapat menikmati konten tersebut.

Penggunaan aplikasi Android pada sistem akses konten untuk mengakses konten digital dapat meningkatkan keamanan konten digital. Dengan menggunakan fitur aplikasi yang menghalangi tangkapan layar, konten digital karya anggota Genshiken ITB dapat terlindungi dari pencurian konten dan duplikasi dengan kualitas tinggi secara ilegal.

Penggunaan aplikasi Android pengguna konten yang memberikan kemudahan pada pengguna dapat meningkatkan penyebaran konten. Pengguna dapat dengan mudah melihat daftar konten digital dan mengakses konten digital yang diinginkan. Dengan kemudahan tersebut, pengguna aplikasi Android dapat mengakses konten digital karya anggota Genshiken ITB sehingga penyebaran konten digital meningkat.

REFERENCES

[1] K. Nagao, Digital Content Annotation and Transcoding Artech, 2003.

[2] A. J., ""How Watermarking Add Value to Digital Content," Communications of the ACM, Vol. 41, Issue 7, pp. 75-77, 1998.

[3] Genshiken ITB, "Tentang Genshiken," 2024. [Online]. Available: https://genshiken-itb.org/about-us. [Accessed 22 Juni 2024].

[4] A. Hamza and B. Kumar, "A Review Paper on DES, AES, RSA Encryption Standards," 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), pp. 333-338, 2020.

[5] Federal Information Processing Standards, Advanced Encryption Standard (AES), 2001.

[6] E. Fernando, D. Agustin, M. Irsan, D. F. Murad, H. Rohayani and D. Sujana, "Performance Comparison of Symmetries Encryption Algorithm AES and DES With Raspberry Pi," in 2019 International Conference on Sustainable Information Engineering and Technology (SI

[7] L. Zheng, R. Chen and X. Cheng, "Research and implementation of digital rights management model for vector graphics," 2011 International Conference on Uncertainty Reasoning and Knowledge Engineering, pp. 17-20, 2011.

[8] [8] V. M. T, R. K. C and R. M E, "Selective Encryption of the Audio Extracted from the Video Streamed Over the Content Delivery Network," in 2021 IEEE Mysore Sub Section International Conference (MysuruCon), Hassan, 2021.