PEMBANGUNAN SISTEM DIGITAL PUBLISHING SEBAGAI SARANA DISTRIBUSI KONTEN INTERAKTIF DI PUSAT MIKROELEKTRONIKA ITB

Andri Setiawan

Teknik Informatika – Universitas Komputer Indonesia
Jl. Dipatiukur 112-114 Bandung
E-mail : dark.siswa@gmail.com

ABSTRAK

Pusat Mikroelektronika merupakan pusat penelitian di bawah ITB yang dikoordinasikan oleh Kantor Wakil Rektor Bidang Riset dan Inovasi. Salah satu produk yang dihasilkan adalah produk informasi berupa konten digital interaktif. Namun saat ini tahapan proses pengembangan konten digital interaktif baru sebatas *authoring*, sehingga proses distribusi dan *viewing* tidak berjalan dengan baik.

Oleh karena itu dibangun sistem digital *publishing* ini yang menggunakan algoritma AES untuk keamanan dan DEFLATE untuk kompresi dari konten yang dihasilkan, sehingga diharapkan dapat membantu proses distribusi dari konten digital interaktif yang dihasilkan.

Berdasarkan hasil pengujian, sistem yang dibangun ini dapat menjadi pendukung proses distribusi dan *viewing* pada sisi pengguna, sehingga proses distribusi konten, keamanan konten, dan proses pembacaan konten dapat berjalan dengan baik dan optimal.

Kata kunci : Digital *Publishing*, Digital *Right Management*, AES, DEFLATE.

1. PENDAHULUAN

Untuk mempublikasi konten digital ada beberapa tahapan yang diperlukan yakni, tahapan produksi (*authoring*), distribusi melalui server konten, dan *viewing* dari sisi pengguna. Namun saat ini tahapan proses pengembangan konten digital interaktif baru sebatas *authoring*, sehingga proses distribusi dan *viewing* tidak berjalan dengan baik. Hal ini dikarenakan belum adanya dukungan sistem publikasi konten digital interaktif.

Untuk menanggulangi masalah tersebut dibutuhkan suatu sistem yang dapat mempublikasikan konten-konten digital dari buku, artikel, management dan media. Sehingga dipilih alternatif membangun sendiri sebuah sistem digital publishing, yang dapat mencakup publikasi digital dari buku, artikel elektronik, dan pengembangan dari perpustakaan digital dan katalog digital serta media pembaca [1].

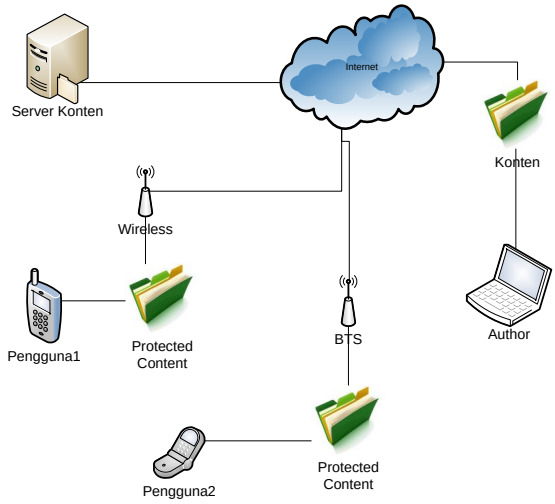
Dari beberapa penjelasan diatas maka terbentuk penelitian dengan judul "**PEMBANGUNAN SISTEM DIGITAL PUBLISHING SEBAGAI SARANA DISTRIBUSI KONTEN INTERAKTIF DI PUSAT MIKROELEKTRONIKA ITB**". Selanjutnya *output* yang diharapkan dalam penelitian ini adalah menghasilkan sebuah produk berupa sistem digital publishing yang terdiri dari server konten berbasis web (*backend*) dan aplikasi *reader* berbasis mobile android (*frontend*), dan memiliki fitur proteksi berupa enrkipsi dan kompresi. Sehingga diharapkan dapat membantu proses distribusi konten interaktif dengan baik.

Maksud dari penulisan tugas akhir ini adalah untuk membangun sistem digital publishing dengan model frontend dan backend, dimana frontend berbasis mobile sebagai media pembaca dan pe-download konten bagi pengguna, dan backend berupa aplikasi web yang berfungsi untuk portal *author* mengunggah konten, dan sebagai sarana distribusi konten digitial interaktif yang dihasilkan oleh pusat mikroelektronika ITB.

2. Sistem yang dibangun

2.1 Arsitektur Sistem

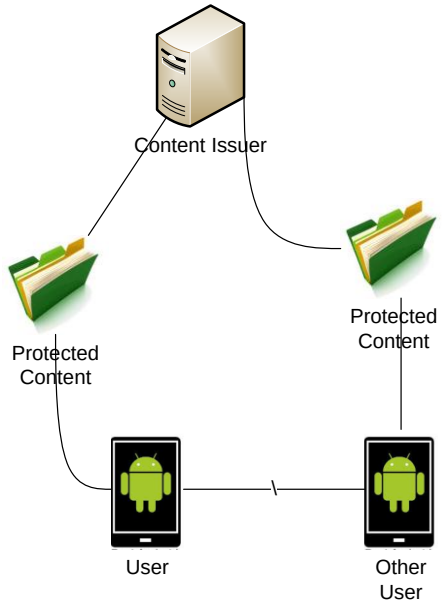
Arsitektur sistem terdiri dari dua komponen utama yaitu *frontend* berbasis *mobile* android, dan *backend* berupa server konten yang merupakan portal untuk *author*. Arsitektur sistem dalam pembangunan sistem ini ditunjukan oleh gambar 1.



Gambar 1. Arsitektur Sistem

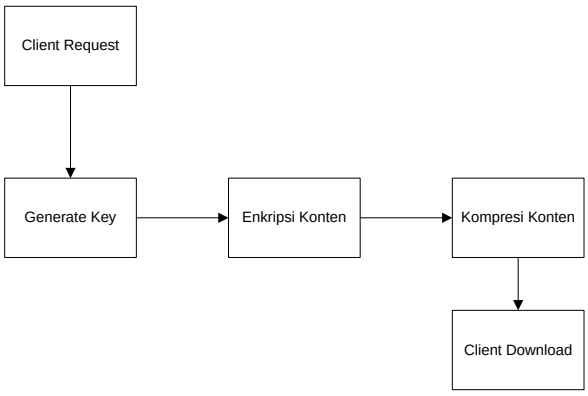
2.1 Digital Right Management

Digital Right Management atau DRM adalah teknologi yang memungkinkan provider konten untuk mendistribusikan konten digital dalam cara yang aman. Pada sistem yang akan dibangun sendiri DRM berfungsi untuk membatasi penggunaan konten, dimana konten hanya dapat ditampilkan pada perangkat yang sudah mendownload konten dari server konten, sehingga konten yang berasal dari proses peng-*copy*-an konten dari pengguna lain tidak akan dapat dibaca.



Gambar 2. Ekosistem DRM

Pada sistem yang akan dibangun, proses DRM dimulai dengan proses *upload* konten dari author, dimana konten yang di*upload*kan sudah terkompresi dengan kompresi zip, kemudian sistem akan mengekstrasi konten tersebut dan kemudian mengenkripsinya sesuai dengan permintaan dari pengguna.



Gambar 3. Proses DRM pada sistem

1. Client Request

Pada bagian ini aplikasi pembaca akan melakukan permintaan untuk men*download* konten. Proses permintaan dilakukan seperti permintaan HTTP pada umumnya.

2. Generate Key

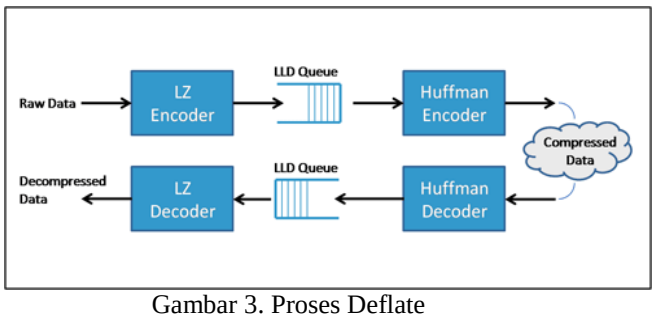
Proses ini akan menghasilkan kunci unik untuk AES.

3. Enkripsi Konten

parameter yang digunakan adalah kunci yang dihasilkan pada proses *generate key*, yang kemudian akan mengenkripsi konten misalnya "index.html" sebagai masukannya dan menghasilkan konten baru terenkripsi dengan nama "index.html.enc".

2.1.2 Deflate

Kompresi DEFLATE yang merupakan kompresi data lossless yang menggunakan kombinasi dari teknik kompresi LZ77 dan Huffman coding. Efisiensi kompresi DEFLATE ini adalah variabel berdasarkan aliran data terkompresi, dan tolak ukur umum menggunakan file berbasis teks menunjukkan rasio kompresi dari 2,5:1 sampai kisaran 3,5:1. Kompresi sebesar ini memiliki keunggulan operasional yang jelas di penyimpanan data dan data jaringan.



Gambar 3. Proses Deflate

Data mentah masuk ke encoder LZ dimana pencocokan string dilakukan dengan menggunakan algoritma hash, tabel hash, dan history buffer. Output dari encoder LZ adalah antrian yang disebut

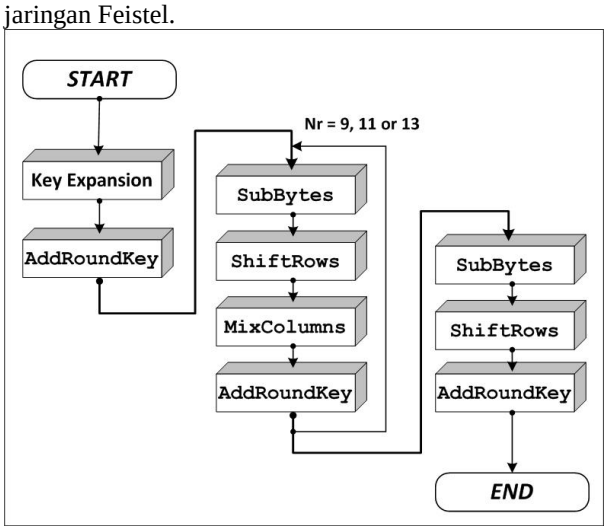
antrian LLD (literals and long / distance), yang menyimpan symbol-simbol yang dihasilkan selama tahap pengkodean LZ. Output dari antrian LLD diproses oleh encoder Huffman yang menghasilkan aliran bit terkompresi.

Pada proses dekompresi, data yang terkompresi diterjemahkan pada decoder Huffman untuk membangun aliran simbol yang dibutuhkan oleh decoder LZ. Decoder LZ beroperasi langsung mematikan aliran simbol tersebut untuk merekonstruksi data asli, dan tidak memerlukan hashing atau tabel hash.

2.1.2 AES

AES atau Advanced Encryption Standard merupakan spesifikasi untuk enkripsi data elektronik yang dibentuk oleh National Institute of Standards and Technology (NIST) pada tahun 2001, dimana standar ini merupakan varian dari algoritma Rijndael, yang merupakan blok cipher simetris yang dapat mengolah data blok 128 bit, menggunakan kunci cipher dengan panjang 128, 192, dan 256 bit.

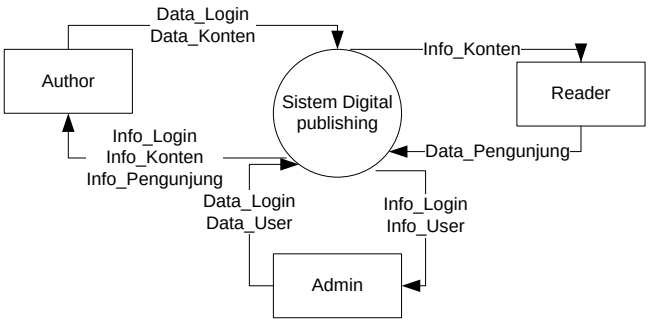
AES didasarkan pada prinsip desain yang dikenal sebagai jaringan substitusi-permutasi, dan penggunaannya cepat dalam perangkat keras maupun perangkat lunak. Tidak seperti pendahulunya DES, AES tidak menggunakan jaringan Feistel.



Gambar 4. Proses AES

2.2 Diagram Konteks

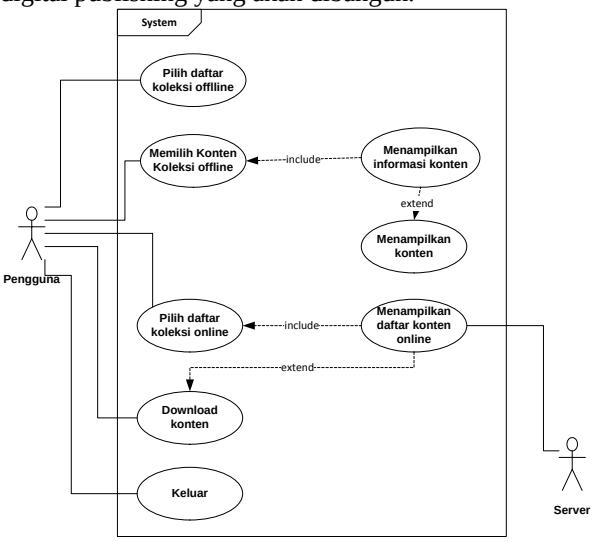
Diagram konteks merupakan suatu penggambaran guna melihat hubungan antara entitas dalam maupun entitas luar pada sistem yang akan dibuat. Dengan adanya diagram konteks diharapkan proses perancangan sistem akan sesuai dengan kenyataan yang terjadi pada sistem.



Gambar 5. Diagram Konteks

2.3 Usecase Diagram

Pemodelan *usecase* adalah pemodelan sistem dari perspektif pandangan pemakai akhir (*end user*). Model *usecase* adalah pandangan dari luar sistem, sementara model rancangan adalah pandangan dari dalam. Model *usecase* menangkap penggunaan-penggunaan sistem, sedangkan model rancangan merepresentasikan pembangunan dari sistem. Berikut ini adalah gambar dari *usecase* untuk sistem digital publishing yang akan dibangun.



Gambar 6. Diagram Konteks

2.4 Analisis Perangkat Keras / Hardware

Analisis kebutuhan nonfungsional dari segi perangkat keras yaitu perangkat keras fitur pendukung aplikasi. Untuk perangkat keras fitur pendukung aplikasi dapat dilihat pada Tabel.

Tabel 1. Perangkat keras *frontend*

No	Perangkat Keras	Spesifikasi
1	Layar	Touchscreen, Multitouch
2	Baterai	Standard
3	Speaker	Standard

4	Processor	1Ghz
5	RAM	1GB
6	Lain-lain	Accelerometer

Tabel 2. Perangkat keras *backend*

No	Perangkat Keras	Spesifikasi
1	Processor	2.0Ghz Dual Core
2	RAM	2GB
3	Harddisk	100GB
4	Network	Gigabyte Ethernet

2.4 Implementasi Perangkat Lunak

Spesifikasi perangkat lunak (software) yang digunakan dalam membangun sistem digital *publishing* ini dapat dilihat pada tabel.

Tabel 1. Tabel perangkat lunak yang digunakan

Jenis	Perangkat Lunak
Sistem Operasi	Microsoft windows 7 Professional
Database Server	MySql
WebServer	Apache2
IDE	Eclipse 4.2.2

2.5 Implementasi Perangkat Keras

Kebutuhan minimum perangkat keras (hardware) yang diperlukan untuk membangun sistem digital *publishing* ini dapat dilihat pada tabel.

Tabel 2. Tabel perangkat keras yang digunakan

Jenis	Perangkat Keras
Processor	Inter Core i5, 25GHz
RAM	4GB
Harddisk	250GB
VGA	1GB

3. Kesimpulan

Berdasarkan hasil pengujian, sistem yang dibangun ini dapat menjadi pendukung proses distribusi dan *viewing* pada sisi pengguna, sehingga proses distribusi konten, keamanan konten, dan proses pembacaan konten dapat berjalan dengan baik dan optimal.

Selanjutnya saran untuk pengembangan selanjutnya dari sistem yang akan dibangun ini adalah desain antarmuka *frontend* yang perlu dikembangkan lagi agar lebih menarik, dan pengoptimasian algoritma kompresi yang digunakan sehingga proses kompresi dapat dilakukan lebih cepat.

DAFTAR PUSTAKA

[1] Thomas Woll, 2010, *Publishing for Profit : Fourth Edition*, New Yorks:Chicago Review Press

[2] Roger, S. Pressman, Ph.D. , 2012, Rekayasa Perangkat Lunak (Pendekatan Praktisi) Edisi 7 : Buku 1, ANDI

[3] Patrick Behar, 2011, *Publishing in the digital era*, New York:Bain and Company

[4] *Object Management Group*, 2006, *Unified Modeling Language: Infrastructure*, Needham, *Object Management Group.*

[5] M. A. P. Jogiyanto HM., Analisis & Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis, Yogyakarta: Andi, 2005.