Skema Kontrol Akses Berbasis Kriptografi untuk Konten Digital Berlangganan

Ahmad Farid Mudrika - 13522008[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]faridm0741@gmail.com

***Abstrak*— Model distribusi konten digital berbasis langganan telah menjadi pendekatan dominan dalam penyediaan perangkat lunak, media, dan data digital. Namun, model ini menimbulkan permasalahan terkait kontrol akses dan kepemilikan konten, khususnya ketika pengguna telah memperoleh salinan penuh dari konten tersebut. Makalah ini mengusulkan sebuah skema kontrol akses berbasis kriptografi yang menggabungkan enkripsi statis terhadap konten dengan rotasi kunci berbasis waktu. Konten digital dienkripsi satu kali menggunakan kunci konten, sementara akses pengguna dikendalikan melalui kunci langganan yang diperbarui secara periodik tanpa memodifikasi berkas terenkripsi.**

Kata Kunci — kriptografi, kontrol akses, rotasi kunci, enkripsi konten digital, sistem berlangganan..

I. Pengenalan

Perkembangan teknologi distribusi digital telah mengubah cara pengguna memperoleh dan mengonsumsi konten, mulai dari perangkat lunak, musik, video, hingga data digital lainnya. Dalam beberapa tahun terakhir, model distribusi berbasis langganan (subscription-based) semakin banyak digunakan karena memberikan fleksibilitas bagi penyedia layanan dalam mengelola pembaruan, lisensi, dan pendapatan berkelanjutan. Namun, model ini juga memunculkan perdebatan terkait konsep kepemilikan digital, terutama ketika pengguna tidak lagi memiliki akses terhadap konten setelah langganan berakhir atau layanan dihentikan.

Salah satu ungkapan yang sering muncul dalam diskusi mengenai kepemilikan digital adalah "if buying isn't owning, then piracy isn't stealing". Pernyataan tersebut mencerminkan ketidakpuasan sebagian pengguna terhadap sistem distribusi digital modern yang membatasi akses meskipun pengguna telah melakukan pembayaran. Permasalahan ini menunjukkan adanya ketegangan antara kepentingan penyedia layanan dalam mengendalikan distribusi konten dan hak pengguna untuk memperoleh kepastian akses terhadap konten yang telah dibeli.

Dari sudut pandang teknis, pembatasan akses terhadap konten digital umumnya dilakukan melalui mekanisme kontrol akses berbasis server atau sistem Digital Rights Management (DRM). Namun, pendekatan tersebut sering kali bergantung pada infrastruktur terpusat dan tidak memberikan jaminan akses jangka panjang kepada pengguna, khususnya jika layanan berhenti beroperasi. Selain itu, sistem DRM yang kompleks cenderung sulit dianalisis secara akademik dan sering menimbulkan resistensi dari pengguna.

Makalah ini mengusulkan pendekatan kontrol akses yang lebih sederhana dan transparan dengan memanfaatkan prinsip-prinsip kriptografi simetris. Konten digital dienkripsi satu kali menggunakan kunci konten, sementara akses pengguna diatur melalui kunci langganan yang diperbarui secara periodik berdasarkan waktu. Dengan pendekatan ini, berkas terenkripsi dapat didistribusikan secara bebas tanpa menghilangkan kontrol akses selama periode langganan masih berlaku. Sebagai tambahan, konsumen dapat merasa lega apabila penyedia konten menjanjikan pelepasan kunci utama ketiak penyedia konten tidak mampu melanjutkan bisnisnya (misalnya, ketika perusahaan penyedia mengalami kebangkrutan).

II. Dasar Teori

A. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) merupakan algoritma kriptografi simetris yang paling banyak digunakan saat ini dan telah distandardisasi oleh National Institute of Standards and Technology (NIST). AES mendukung panjang kunci 128, 192, dan 256 bit, dengan tingkat keamanan yang dianggap memadai untuk penggunaan komersial maupun akademik.

AES bekerja dengan memproses data dalam blok berukuran 128 bit dan menerapkan sejumlah transformasi matematis, seperti substitusi byte, permutasi baris, dan operasi aljabar pada medan hingga. Dalam praktik, AES umumnya digunakan dalam berbagai mode operasi seperti Cipher Block Chaining (CBC) atau Galois/Counter Mode (GCM) untuk meningkatkan keamanan dan fleksibilitas penggunaan.

Dalam konteks makalah ini, AES digunakan untuk mengenkripsi konten digital secara statis, sehingga berkas terenkripsi tidak perlu diubah selama masa distribusi.

B. Manajemen Kunci Kriptografi

Manajemen kunci merupakan aspek krusial dalam sistem kriptografi, yang mencakup proses pembuatan, penyimpanan, distribusi, rotasi, dan penghancuran kunci. Keamanan suatu sistem enkripsi sering kali lebih ditentukan oleh bagaimana kunci dikelola dibandingkan dengan algoritma enkripsinya sendiri.

Pada sistem distribusi konten digital, manajemen kunci digunakan untuk membatasi siapa saja yang dapat mengakses konten dan dalam periode waktu tertentu. Dengan memisahkan kunci enkripsi konten dari kunci akses pengguna, sistem dapat menerapkan kontrol akses yang lebih fleksibel tanpa harus melakukan enkripsi ulang terhadap konten secara keseluruhan.

C. Rotasi Kunci

Rotasi kunci (key rotation) adalah teknik keamanan yang mengganti kunci kriptografi secara berkala untuk mengurangi risiko penyalahgunaan kunci yang telah bocor atau digunakan terlalu lama. Rotasi kunci dapat dilakukan berdasarkan jumlah penggunaan, peristiwa tertentu, atau periode waktu.

Dalam pendekatan berbasis waktu, kunci hanya berlaku untuk interval tertentu, seperti harian atau bulanan. Setelah periode tersebut berakhir, kunci lama tidak lagi digunakan dan digantikan oleh kunci baru. Pendekatan ini umum digunakan pada sistem autentikasi dan kontrol akses karena relatif sederhana dan mudah diimplementasikan.

Makalah ini menggunakan konsep rotasi kunci berbasis waktu untuk mengendalikan akses konten digital dalam sistem berlangganan, di mana kunci akses diperbarui setiap periode tertentu tanpa mengubah berkas terenkripsi.

D. Envelope Encryption

Envelope encryption merupakan teknik enkripsi berlapis yang memisahkan antara kunci konten (content key) dan kunci akses (key encryption key). Dalam skema ini, data atau konten dienkripsi menggunakan kunci konten, sedangkan kunci konten tersebut dienkripsi kembali menggunakan kunci lain yang berfungsi sebagai pengendali akses.

Keuntungan utama dari envelope encryption adalah efisiensi dan fleksibilitas. Konten berukuran besar tidak perlu dienkripsi ulang ketika terjadi perubahan kebijakan akses; cukup dengan mengenkripsi ulang kunci konten menggunakan kunci akses yang baru. Teknik ini banyak digunakan pada sistem penyimpanan awan dan layanan manajemen kunci modern.

Pendekatan yang diusulkan dalam makalah ini mengadopsi prinsip envelope encryption untuk memungkinkan perubahan kunci langganan secara periodik tanpa memodifikasi berkas konten yang telah dienkripsi.

III. METODOLOGI

A. Skema Enkripsi

Skema yang diusulkan menggunakan dua jenis kunci, yaitu kunci konten dan kunci langganan.

1. Kunci Konten (Content Key)

   Kunci konten digunakan untuk mengenkripsi berkas digital secara langsung menggunakan algoritma kriptografi simetris. Kunci ini bersifat statis dan tidak berubah selama masa distribusi konten.

2. Kunci Langganan (Subscription Key)

   Kunci langganan digunakan untuk mengenkripsi kunci konten dan diperbarui secara periodik berdasarkan periode waktu tertentu, misalnya bulanan. Kunci ini dihasilkan melalui proses derivasi kunci yang melibatkan rahasia utama dan parameter periode waktu.

Dengan pemisahan ini, berkas terenkripsi tidak perlu diubah ketika masa berlaku langganan berubah, karena hanya kunci konten yang dienkripsi ulang menggunakan kunci langganan yang baru..

B. Derivasi Kunci Berbasis Waktu

Derivasi kunci langganan dilakukan dengan menggabungkan rahasia utama sistem dan parameter periode waktu. Parameter waktu direpresentasikan dalam bentuk jendela waktu diskret, misalnya tahun dan bulan aktif. Proses ini menghasilkan kunci yang berbeda untuk setiap periode tanpa perlu menyimpan seluruh kunci secara eksplisit.

Secara konseptual, kunci langganan dihasilkan sebagai berikut:

$$K_{sub} = H(K_{master} \parallel T)$$

dengan $H(\cdot)$ merupakan fungsi hash kriptografis, K_{master} adalah rahasia utama sistem, dan T adalah representasi periode waktu aktif.

IV. PEMBAHASAN

Eksperimen dilakukan dengan mengenkripsi sebuah berkas digital menggunakan kunci konten statis dan kunci langganan berbasis periode waktu bulanan. Pengujian difokuskan pada kemampuan sistem dalam membatasi akses konten berdasarkan perubahan periode waktu tanpa memodifikasi berkas terenkripsi.

Pada periode waktu yang sesuai, proses dekripsi kunci konten menggunakan kunci langganan berhasil dilakukan, sehingga berkas konten dapat didekripsi dan diakses secara normal. Sebaliknya, ketika periode waktu diubah ke periode berikutnya, proses dekripsi kunci konten gagal karena kunci langganan yang dihasilkan berbeda dari periode sebelumnya. Akibatnya, berkas konten tidak dapat didekripsi meskipun berkas terenkripsi tetap sama.

Hasil ini menunjukkan bahwa rotasi kunci berbasis waktu mampu mengendalikan akses konten secara efektif tanpa memerlukan enkripsi ulang terhadap berkas konten. Dengan demikian, sistem memenuhi tujuan utama perancangan, yaitu pemisahan antara distribusi berkas dan kontrol akses.

Skema yang diusulkan juga memiliki implikasi terhadap konsep kepemilikan digital. Dengan menyediakan mekanisme pelepasan kunci utama apabila layanan berhenti beroperasi, sistem memberikan jaminan akses jangka panjang kepada pengguna terhadap konten yang telah dibeli. Pendekatan ini dapat dipandang sebagai kompromi antara kontrol distribusi oleh penyedia layanan dan hak pengguna atas konten digital.

Meskipun mekanisme ini bergantung pada kepercayaan terhadap penyedia layanan, penyertaan konsep pelepasan kunci utama menunjukkan bahwa kriptografi dapat digunakan tidak hanya sebagai alat pengamanan teknis, tetapi juga sebagai sarana untuk mendukung prinsip keadilan dan transparansi dalam distribusi konten digital. Untuk menghilangkan kebergantungan pada kepercayaan terhadap penyedia layanan, penyedia layanan dapat menyediakan *smart contract* berbasis blockchain yang akan melepaskan kunci utama ketika penyedia layanan berhenti beroperasi.

Meskipun menunjukkan hasil yang sesuai dengan tujuan perancangan, sistem yang diusulkan memiliki sejumlah keterbatasan. Pertama, sistem ini tidak mencegah pengguna menyimpan salinan konten dalam bentuk tidak terenkripsi setelah berhasil melakukan dekripsi. Oleh karena itu,

pendekatan ini tidak dapat dianggap sebagai sistem Digital Rights Management (DRM) penuh.

Kedua, sistem bergantung pada mekanisme distribusi kunci langganan yang aman. Apabila kunci langganan atau rahasia utama bocor, maka kontrol akses tidak lagi dapat dijamin. Selain itu, penggunaan waktu lokal sebagai parameter derivasi kunci berpotensi dimanipulasi oleh pengguna, kecuali jika dikombinasikan dengan sumber waktu tepercaya.

V. Kesimpulan

A. Kesimpulan

Hasil pembahasan menunjukkan bahwa pendekatan ini mampu memisahkan antara proses enkripsi konten dan mekanisme pengendalian akses berbasis waktu, sehingga rotasi kunci dapat dilakukan dengan biaya komputasi yang rendah. Selain itu, skema ini memungkinkan adanya mekanisme pelepasan kunci utama sebagai bentuk perlindungan konsumen apabila penyedia layanan berhenti beroperasi, tanpa memerlukan perubahan terhadap konten yang telah didistribusikan.

Namun demikian, pendekatan yang diusulkan memiliki keterbatasan inheren. Apabila pengguna menyimpan kunci langganan dari periode sebelumnya, maka akses terhadap konten tetap dapat dilakukan meskipun langganan telah berakhir. Oleh karena itu, skema ini tidak dimaksudkan sebagai solusi pencabutan akses yang bersifat absolut, melainkan sebagai mekanisme pengaturan distribusi kunci berbasis waktu. Keterbatasan ini merupakan konsekuensi dari asumsi distribusi konten dan kunci secara offline tanpa ketergantungan pada sistem terpusat.

B. Saran

Untuk pengembangan selanjutnya, penulis menyarankan hal berikut:

1. Implementasi sistem penyebaran kunci dan dekripsi konten, sehingga pengguna tidak memiliki akses ke kunci langganan.
2. Implementasi sistem keamanan tambahan, seperti penghapusan konten yang didistribusi jika pengguna tidak memperpanjang langganan.

VI. Ucapan Terima Kasih

Penulis ingin menyampaikan rasa terima kasih yang tulus kepada beberapa pihak atas kontribusi mereka terhadap makalah ini. Pertama-tama, penulis menyampaikan rasa syukur yang mendalam kepada Allah yang telah memberikan petunjuk selama proses belajar dan penulisan. Selain itu, penulis juga mengakui dukungan dan pengajaran yang sangat berharga yang diterima dari dosen Kriptografi IF4020 ITB, Bapak Rinaldi Munir. Pengetahuan dan bimbingannya telah memperkaya pengalaman belajar di kelas secara signifikan. Ucapan terima kasih yang istimewa juga ditujukan kepada keluarga dan teman-teman penulis atas dukungan mereka yang tak tergoyahkan sepanjang semester ini.

Pranala Github

Kode yang digunakan dan data yang lebih lengkap dapat dilihat di:

https://github.com/frdmmm/kripto_makalah

Daftar Pustaka

[1] https://informatika.stei.itb.ac.id/~rinaldi.munir/Citra/2025-2026/22-Segmentasi-Citra-Bagian1-2025.pdf

[2] https://informatika.stei.itb.ac.id/~rinaldi.munir/Citra/2025-2026/23-Segmentasi-Citra-Bagian2-2025.pdf

[3] https://docs.pytorch.org/vision/main/models/deeplabv3.html

Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 26 Desember 2025

Ahmad Farid Mudrika 13522008