ISSN: 2598-8565 (media cetak)
ISSN: 2620-4339 (media online)

KONSEP PENGAMANAN VIDEO CONFERENCE DENGAN ENKRIPSI AES-GCM PADA APLIKASI ZOOM

[1]Jamaluddin✉, [2]Naikson Fandier Saragih, [1]Roni Jhonson Simamora, [1]Rimbun Siringoringo, [3]Eviyanti Novita Purba
[1]Program Studi Manajemen Informatika, Universitas Methodist Indonesia, Medan, Indonesia
[2]Program Studi Teknik Informatika, Universitas Methodist Indonesia, Medan, Indonesia
[3]Program Studi Komputerisasi Akuntansi, Universitas Methodist Indonesia, Medan, Indonesia
Email: jamaluddin@methodist.ac.id

DOI: https://doi.org/10.46880/jmika.Vol4No2.pp109-113

ABSTRACT

The conditions of the Covid-19 pandemic, which began to plague at the end of 2019, brought about major changes to the patterns of interaction in society. Activities that have been carried out directly have begun to shift to activities carried out online. The use of technology, especially in applications for online interaction patterns such as video conferencing applications, is an alternative. The Zoom Cloud Meeting application is widely used by people who initially had doubts about its security system. By implementing end-to-end encryption with AES-256-GCM, it has been able to convince clients on the information security side to keep using the Zoom Cloud Meeting application.

Keyword: Zoom Cloud Meeting, AES-256-GCM, Pandemic Covid-19.

ABSTRAK

Kondisi pandemi Covid-19 yang mulai mewabah pada akhir tahun 2019 membawa perubahan yang besar pada pola interaksi di masyarakat. Kegiatan yang selama ini dilakukan secara langsung mulai beralih ke kegiatan yang dilakukan secara daring. Pemanfaatan teknologi, khususnya pada aplikasi untuk pola interaksi daring seperti aplikasi *video conference* menjadi alternatif. Aplikasi *Zoom Cloud Meeting* yang banyak digunakan oleh masyarakat yang pada awalnya diragukan sistem keamanannya. Dengan penerapan enkripsi *end-to-end* dengan AES-256-GCM telah mampu meyakinkan klien pada sisi keamanan informasi untuk tetap menggunakan aplikasi *Zoom Cloud Meeting*.

Kata Kunci: Aplikasi Zoom, AES-256-GCM, Pandemi Covid-19.

PENDAHULUAN

Pada akhir tahun 2019, sebuah virus korona yang belum teridentifikasi sebelumnya muncul di kota Wuhan, Tiongkok. Virus korona ini, yang sekarang dikenal sebagai Covid-19, menyebar dengan cepat secara global, seperti penyebaran virus korona Italia, Spanyol, Russia, Korea Selatan, Jepang, Iran, Filipina, Amerika Serikat, Brasil, India dan juga di Indonesia (WHO, 2020). Kasus pertama di Indonesia diumumkan oleh presiden Joko Widodo pada hari Senin, 2 Maret 2020 yang menginfeksi dua Warga Negara Indonesia (Ihsanuddin, 2020). Perkembangan kasus pasien yang terinfeksi Covid-19 di Indonesia terus meningkat, yang menyebabkan pembatasan terhadap aktivitas masyarakat yang digaungkan dengan tagline #StayAtHome, dimana sebagian besar aktivitas masyarakat dilakukan dari rumah, seperti bekerja dari rumah (*work from home*), belajar dari rumah (*school from home*), ibadah di rumah dan kegiatan-kegiatan lainnya dilakukan dari rumah secara daring (Candra, 2020).

Sistem belajar dari rumah dengan secara daring mulai diterapkan sejak adanya kebijakan pemerintah. Pembelajaran daring adalah sistem belajar tanpa tatap muka langsung, tetapi memakai *platform* yang dapat membantu proses belajar mengajar yang dilakukan secara jarak jauh (Sofyana & Rozaq, 2019). Penerapan sistem pembelajaran daring dilakukan dengan menggunakan *platform* belajar online yang sudah dikembangkan institusi maupun aplikasi pembelajaran yang tersedia, diantaranya *Google Classroom, Edmodo,* Ruang Guru, Rumah Belajar, Meja Kita, *Icando,* Sekolahmu dan IndonesiaX (Handarini & Wulandari, 2020). Selain dari aplikasi tersebut terdapat juga aplikasi yang dapat digunakan secara *video conference* dalam sistem pembelajaran, seperti *Cisco Webex, Zoom* dan *CloudX.*

Penggunaan aplikasi *video conference*,

ISSN: 2598-8565 (media cetak)
ISSN: 2620-4339 (media online)

khususnya *Zoom* juga semakin massif di masa pademi Covid-19 sekarang ini. Penggunaan aplikasi *Zoom* pada kegiatan belajar mengajar harus didukung dengan kualitas jaringan yang baik (Brahma, 2020). Jaminan keamanan pada aplikasi *Zoom* pada awal kemunculannya pada masa pandemic Covid-19 sempat diragukan (Salsabila, 2020). Pengembangan keamanan dilakukan oleh pengembang aplikasi Zoom dengan meningkatkan keamanan enkripsi *End-to-End* (Ikhsan, 2020). Pada artikel ini, penulis tertarik untuk membahas tentang penerapan enkripsi *End-to-End* dengan *AES-GCM* yang ditanamkan pada aplikasi *Zoom*.

TINJAUAN PUSTAKA

Pembelajaran Daring

Menurut Undang-Undang No. 20 Tahun 2003 tentang Sistem Pendidikan Nasional, Pembelajaran daring adalah sistem pembelajaran dimana pendidik dan anak didik terpisah secara fisik dengan menggunakan berbagai sumber belajar melalui media komunikasi jarak jauh dan media lain. Pembelajaran daring dikenal juga sebagai *e-learning*. *E-learning* adalah sistem yang dirancang untuk menghilangkan keterbatasan antara pendidik dan anak didik yang tidak harus berada pada ruang dan waktu yang sama (Kusmana, 2011).

Metode pembelajaran daring dapat dilakukan pada empat komponen pendidikan, yakni pendidikan umum, meningkatkan pengetahuan pendidik tentang materi yang diajarkan, pengajaran pedagogi dan perkembangan anak didik, dan sebagai panduan menuju kelas yang lebih baik (Taufik, 2019). Terdapat enam karakteristik pada pembelajaran daring yakni adanya pemisah diantara pendidik dan anak didik, pengaruh dari institusi pendidikan, penggunaan media yang dapat mengkoneksikan pendidik dan anak didik, terjadinya komunikasi dua arah, memastikan anak didik sebagai individu yang sedang belajar, dan pendidikan sebagai sebuah industri (Keegan, 1980).

Aplikasi *Zoom Cloud Meeting*

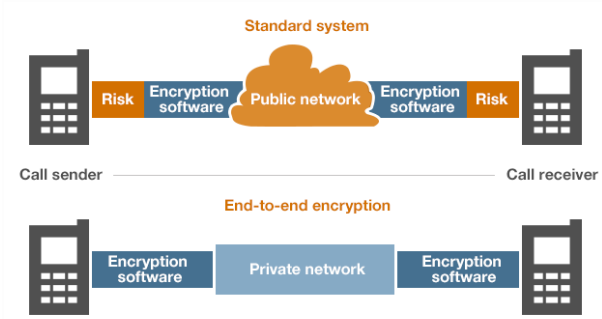
Zoom Cloud Meeting adalah aplikasi yang dapat digunakan untuk komunikasi jarak jauh dengan mengkolaborasikan fitur *video conference*, *chat*, pertemuan online dan kolaborasi seluler. Aplikasi ini dapat menampung hingga 1000 peserta secara bersama dalam suatu pertemuan secara daring. Aplikasi ini juga menyediakan ruang parallel, yang dapat membagi peserta dalam beberapa ruang. Aplikasi ini mendapat penilaian kualitas yang baik dibuktikan dengan banyanya perusahaan yang masuk *fortune 500* yang menggunakan layanan aplikasi ini (Ismawati & Prasetyo, 2020).

Fitur-fitur yang dimiliki pada aplikasi *Zoom* diantaranya pertemuan rapat *one-on-one*, mengelola konferensi ataupun webinar, *sharing screen*, *chat* dan perekaman video. Aplikasi Zoom dapat digunakan secara gratis, tetapi disediakan juga Zoom premium yang memiliki fitur yang lebih lengkap.

Gambar 1. *Meeting* pada Aplikasi *Zoom*

Enkripsi *End-to-End*

Enkripsi *End-to-End* adalah sebuah teknik enkripsi data yang dilakukan pada saat data akan dikirimkan (pengirim) dan kembali didekripsikan pada saat pesan sampai di tujuan (penerima). Pada enkripsi *end-to-end*, paket data dienkripsi sekali pada sumber enkripsi asli dan kemudian didekripsi hanya pada tujuan akhir dekripsi. Perbandingan skema enkripsi End-to-End dan enkripsi standar ditunjukkan pada gambar 2 berikut.



Gambar 2. Perbandingan Sistem Enkripsi Standard dan Sistem Enkripsi *End-to-end*

Keunggulan dari *end-to-end* enkripsi adalah kecepatan dan keamanan secara keseluruhan terhadap data yang dikirimkan. Penggunaan enkripsi End-to-End diantaranya diterapkan pada aplikasi *WhatsApp* (Jamaluddin, Simamora, & Sitepu, 2016) dan *Instant Messaging* (Fahrianto & Kitanggi, 2016).

ISSN: 2598-8565 (media cetak)
ISSN: 2620-4339 (media online)

***Advanced Encryption Standard with Galois Counter Mode* (AES-GCM)**

Advanced Encryption Standard with Galois Counter Mode (AES-GCM) diperkenalkan oleh National Institute for Standar and Technology (NIST). AES merupakan teknik enkripsi yang cocok untuk diterapkan dalam komunikasi ataupun aplikasi elektronik (Pitchaiah, Daniel, & Praveen, 2012). AES-GCM adalah model enkripsi blok yang memberikan kecepatan tinggi pada proses enkripsi terautentikasi dan integrasi data. AES-GCM memiliki dua fungsi utama yakni enkripsi blok cipher dan multiplikasi pada penyandiannya.

Arsitektur AES-GCM dirancang secara paralel agar memiliki kinerja enkripsi dan dekripsi yang lebih tinggi. Algoritma AES-GCM dapat mengenkripsi atau mendekripsi dengan kunci sandi 128-bit, 192-bit atau 256-bit. Arsitektur paralel dari perluasan kunci dirancang saat ukuran kunci yang lebih besar digunakan. Penggunaan ukuran kunci 256-bit akan menyebabkan eksekusi pergantian 14 putaran dan diperlukan permutasi. Ukuran kunci tergantung pada tingkat keamanan yang diinginkan. Jumlah standar putaran transformasi AES-256 adalah empat belas putaran (Ahmad, Wei, & Jabbar, 2018).

METODOLOGI PENELITIAN

Penulisan artikel ini menggunakan metode penelitian kepustakaan yang menggumpulkan informasi dan data dari berbagai macam sumber. Adapun sumber materi pada artikel ini berupa jurnal ilmiah, berita pada koran/majalah, situs internet serta sumber lain yang memiliki relevansi dengan isi artikel ini.

PEMBAHASAN

Konsep pengamanan *Advanced Encryption Standard with Galois Counter Mode* (AES-GCM) merupakan sebuah model pengamanan enkripsi blok yang dirancang secara paralel dengan mengkombinasikan *Advanced Encryption Standard* (AES) dengan *Galois Counter Mode* (GCM). *Galois Counter Mode* (GCM) merupakan model operasi cipher blok yang menggunakan *hash function* melalui Galois biner untuk menerapkan sistem yang diotentikasi. GCM memiliki dua operasi, enkripsi terotentikasi dan dekripsi terotentikasi (McGrew & Viega, 2004).

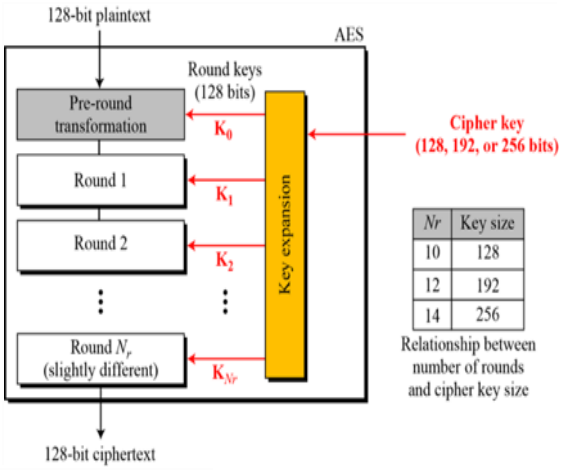
Operasi enkripsi yang diotentikasi memiliki empat input, yang masing-masing berupa:

- Kunci k, yang memiliki panjang sesuai ukuran blok yang digunakan.
- Vektor inisialisasi IV, dengan jumlah bit 1 sampai dengan 2^{64}.
- Plainteks, dengan jumlah bit 0 sampai dengan 256.
- *Additional Authenticated Data* (AAD), dengan jumlah bit 0 dan 2^{64}.

Sedangkan output dari operasi enkripsi terotentikasi yang dihasilkan berupa:

- Cipherteks dengan panjang sama dengan plainteks.
- Tag otentikasi (*an authentication tag*), dengan panjang antara 0 sampai dengan 128 bit.

Advanced Encryption Standard (AES) adalah yang mengenkripsi ataupun mendekripsi secara blok dalam 128bit ataupun 256 bit. AES menggunakan 10, 12 atau 14 putaran untuk sekali proses enkripsi maupun dekripsi. Kunci yang digunakan untuk proses enkripsi maupun dekripsi bisa 128, 192 atau 256bit yang bergantung dari jumlah putaran.



Nr	Key size
10	128
12	192
14	256

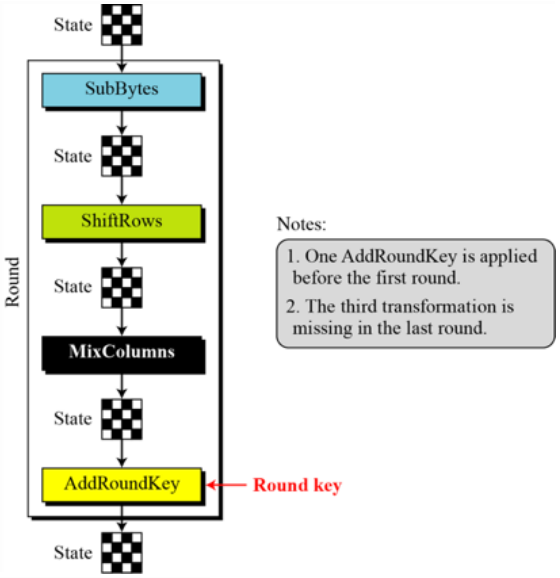
Relationship between number of rounds and cipher key size

Sumber: (Forouzan, 2007)

Gambar 3. Proses Enkripsi AES

Untuk memberikan keamanan, pada setiap putarannya AES menggunakan empat jenis transformasi yakni subsitusi, permutasi, pencampuran dan penjumlahan dengan kunci, seperti ditampilkan pada gambar 4. Empat jenis transformasi yang digunakan pada AES pada standarnya untuk algoritma enkripsi disebut sebagai sandi dan pada algoritma dekripsinya disebut sandi terbalik.

ISSN: 2598-8565 (media cetak)
ISSN: 2620-4339 (media online)

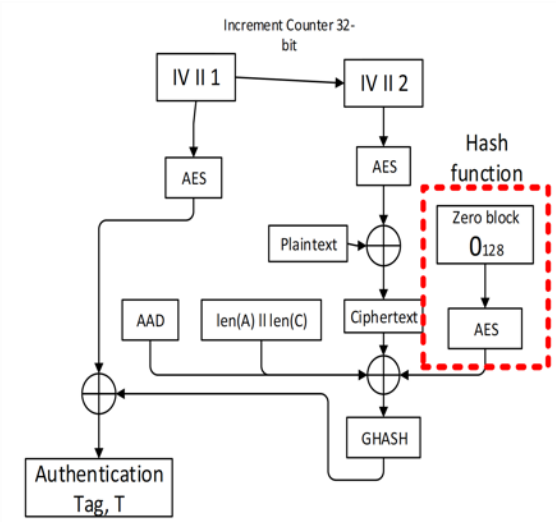


Sumber: (Forouzan, 2007)

Gambar 4. Skema Proses Enkripsi AES pada setiap putarannya

AES dapat diimplementasikan pada software maupun hardware. Implementasinya dapat menggunakan proses atau rutinitas yang menggunakan struktur aljabar yang terdefinisi dengan baik. Pengimplementasikan AES juga dapat dikombinasikan dengan teknik ataupun algoritma yang lain, salah satu yang dibahasi pada artikel ini adalah pengkombinasian AES dengan GCM.

AES-GCM memiliki dua komponen utama yakni mesin AES dan fungsi GHASH seperti terlihat pada gambar 5. Fungsi GHASH diterapkan untuk menghasilkan satu blok output dimana hasilnya dipotong ke panjang tag yang ditentukan untuk membentuk tag otentikasi.



Sumber: (Ahmad et al., 2018)

Gambar 5. Skema Enkripsi dan Dekripsi AES-GCM

Penerapan enkripsi AES-256-GCM pada aplikasi Zoom dimulai pada tanggal 30 Mei 2020 untuk semua perangkat yang menggunakan aplikasi Zoom versi 5.x pada perangkat klien. Langkah ini diambil untuk meningkatkan keamanan bagi klien dan juga memastikan klien menggunakan aplikasi Zoom versi terbaru. Pada pembaharuan tingkat keamanan ini, aplikasi Zoom menyertakan kemampuan untuk melihat tingkat enkripsi yang terjadi pada saat panggilan sedang berlangsung, seperti ditunjukkan pada gambar berikut:

Gambar 6. Statistik pada Zoom dengan enkripsi AES-256-GCM

KESIMPULAN

Pemanfaatan aplikasi *Zoom Cloud Meeting* sebagai aplikasi *video conference* pada masa pandemi Covid-19 meningkat secara pesat. Permasalahan keamanan pada aplikasi *Zoom Cloud Meeting* pada masa awal pandemic Covid-19 telah ditindaklanjuti dengan penggunaan enkripsi AES-256-GCM dengan teknik *End-to-End.* Dengan sistem enkripsi *End-to-End* dengan AES-256-GCM maka data dari klien akan dapat lebih terjamin pada aplikasi *Zoom Cloud Meeting.*

DAFTAR PUSTAKA

Ahmad, N., Wei, L. M., & Jabbar, M. H. (2018). Advanced Encryption Standard with Galois Counter Mode using Field Programmable Gate Array. *Journal of Physics: Conference Series*, *1019*(1), 1–7. https://doi.org/10.1088/1742-6596/1019/1/012008

Brahma, I. A. (2020). Penggunaan Zoom Sebagai Pembelajaran Berbasis Online Dalam Mata Kuliah Sosiologi dan Antropologi Pada Mahasiswa PPKN di STKIP Kusumanegara Jakarta. *Aksara: Jurnal Ilmu Pendidikan Nonformal*, *6*(2), 97.

https://doi.org/10.37905/aksara.6.2.97-102.2020

Candra, S. A. (2020, March 15). Jokowi: Saatnya Kerja, Belajar, Ibadah di Rumah. *Republika*. Retrieved from https://republika.co.id/

Fahrianto, F., & Kitanggi, A. (2016). Penerapan End-To-End Encryption Dengan Metode Super Encryption Untuk Kerahasiaan Citra Digital Pada Aplikasi Instant Messaging. *Jurnal Teknik Informatika*, *9*(1), 1–8. https://doi.org/10.15408/jti.v9i1.5651

Forouzan, B. A. (2007). *Cryptography & Network Security*. New York: McGraw-Hill Education.

Handarini, O. I., & Wulandari, S. S. (2020). Pembelajaran Daring Sebagai Upaya Study From Home (SFH) Selama Pandemi Covid 19. *Jurnal Pendidikan Administrasi Perkantoran (JPAP)*, *8*(3), 496–503.

Ihsanuddin. (2020, March 2). BREAKING NEWS: Jokowi Umumkan Dua Orang di Indonesia Positif Corona. *Kompas.Com*. Retrieved from https://nasional.kompas.com/

Ikhsan, M. (2020, May 11). Zoom Klaim Tingkatkan Keamanan Enkripsi "end-to-end." *CNN Indonesia*. Retrieved from https://www.cnnindonesia.com/

Ismawati, D., & Prasetyo, I. (2020). Efektivitas Pembelajaran Menggunakan Video Zoom Cloud Meeting pada Anak Usia Dini Era Pandemi Covid-19. *Jurnal Obsesi : Jurnal Pendidikan Anak Usia Dini*, *5*(1), 665–675. https://doi.org/10.31004/obsesi.v5i1.671

Jamaluddin, J., Simamora, R. J., & Sitepu, K. (2016). Konsep Pengamanan Pesan dengan Teknik Enkripsi End to End pada WhatsApp Messenger. *Jurnal Stindo Profesional*, *9*(1), 177–181. https://doi.org/10.31227/osf.io/hdqtu

Keegan, D. J. (1980). On defining distance education. *Distance Education*, *1*(1), 13–36. https://doi.org/https://doi.org/10.1080/0158791800010102

Kusmana, A. (2011). E-Learning Dalam Pembelajaran. *Lentera Pendidikan : Jurnal Ilmu Tarbiyah Dan Keguruan*, *14*(1), 35–51. https://doi.org/10.24252/lp.2011v14n1a3

McGrew, D., & Viega, J. (2004). The GCM Mode. In *National Institute of Standards and Technology (NIST)*. Retrieved from http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf%5Cnhttp://siswg.net/docs/gcm_spec.pdf

Pitchaiah, M., Daniel, P., & Praveen. (2012). Implementation of Advanced Encryption Standard Algorithm. *International Journal of Scientific & Engineering Research*, *3*(3), 1–6.

Salsabila, P. Z. (2020, April 2). Bahaya yang Mengintai di Balik Penggunaan Zoom. *Kompas.Com*.

Sofyana, L., & Rozaq, A. (2019). Pembelajaran Daring Kombinasi Berbasis Whatsapp Pada Kelas Karyawan Prodi Teknik Informatika Universitas Pgri Madiun. *Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)*, *8*(1), 81. https://doi.org/10.23887/janapati.v8i1.17204

Taufik, A. (2019). Perspektif Tentang Perkembangan Sistem Pembelajaran Jarak Jauh Di Kabupaten Kutai Kartanegara Kalimantan Timur. *Jurnal Pendidikan&Konseptual*, *3*(2), 88–98. https://doi.org/DOI:http://doi.org/10.28926/riset_konseptual.v2i4.111

WHO. (2020). Coronavirus disease (COVID-19) pandemic. Retrieved August 20, 2020, from WHO website: https://www.who.int/