Data Privacy on Zoom amidst COVID-19 Pandemic

Johanes Antonius, 18217036, Sistem dan Teknologi Informasi

Makalah Keamanan Informasi

Abstract---Pandemi COVID-19 menyebabkan banyak keterbatasan dalam bertemu langsung dan berkomunikasi, sehingga dibutuhkan suatu fasilitas yang dapat menggantikan hal tersebut. Konferensi video merupakan salah satu cara untuk menggantikan pertemuan tatap muka secara langsung dengan cukup efektif, dan salah satu aplikasi konferensi video yang populer adalah Zoom karena menawarkan berbagai fungsionalitas. Namun, Zoom juga memiliki banyak isu terkait keamanan dan juga privasi data dari penggunanya.

Keywords---konferensi video, privasi, data, zoom, enkripsi, routing, keamanan informasi

Pendahuluan

Seiring dengan teknologi yang sudah semakin maju, cara manusia melakukan komunikasi juga menjadi semakin beragam. Salah satu cara komunikasi yang sangat sering dilakukan pada zaman sekarang adalah komunikasi jarak jauh, entah melalui pesan, suara, atau video. Meskipun dianggap tidak memiliki efektivitas yang sama dengan komunikasi langsung secara tatap muka, komunikasi jarak jauh merupakan alternatif yang sangat baik karena dapat menghemat waktu dan tenaga yang dibutuhkan untuk bertemu secara langsung.

Berdasarkan berbagai variasi media komunikasi jarak jauh yang tersedia, mayoritas orang menganggap bahwa berkomunikasi dengan menggunakan pesan sudah cukup, misalkan dalam lingkungan kerja profesional komunikasi dilakukan dengan mengirim surat elektronik. Hal ini disebabkan karena mengirim pesan adalah salah satu tindakan yang cukup mudah untuk dilakukan dan dapat menyampaikan maksud dari pengirimnya dengan jelas. Mengirim pesan juga memakan waktu yang relatif singkat jika dibandingkan harus melakukan komunikasi menggunakan suara atau video.

Meskipun demikian, di tengah situasi pandemik COVID-19 yang disebabkan oleh virus Sars-CoV-2 ini, komunikasi jarak jauh menggunakan video, yang biasa disebut dengan konferensi video, menjadi salah satu media yang sangat sering digunakan. Hal ini terjadi karena batasan dan paksaan yang diberlakukan untuk pencegahan penyebaran virus corona, yang dirangkum dalam satu jargon oleh WHO sebagai *physical distancing.* Dengan situasi tersebut yang membuat manusia tidak dapat bertemu secara langsung, berkomunikasi dengan mengirim pesan saja tidak cukup. Sehingga aplikasi seperti Zoom yang menyediakan layanan konferensi video pun menjadi populer.

Zoom sebagai aplikasi sudah dibuat sejak tahun 2011, dan dirilis secara resmi pada tahun 2013. Sejak dirilis Zoom memiliki cukup banyak pengguna, namun tidak sepopuler aplikasi yang menyediakan layanan sama seperti Skype, Google Meet, Slack, dan lain-lain. Beberapa bulan belakangan ini Zoom menjadi sangat populer karena berbagai fitur dan kemudahan yang ditawarkan olehnya, namun bersamaan dengan popularitas yang meningkat tersebut, ada beberapa isu yang timbul terkait keamanan informasi dalam penggunaan Zoom, khususnya terkait privasi data dari pengguna.

Keamanan Informasi dalam Lingkungan Work From Home

Work From Home yang umumnya disingkat sebagai WFH merupakan salah satu istilah yang digunakan untuk aktivitas bekerja yang dilakukan di rumah masing-masing, berbeda dengan aktivitas yang biasanya dilakukan bersama-sama di kantor. Tentunya bekerja di rumah dan bekerja secara konvensional sangatlah berbeda, mulai dari pakaian, jadwal, cara berkomunikasi, serta hal-hal lainnya.

Salah satu aspek vital yang menyangkut keamanan informasi dalam lingkungan kerja adalah cara berkomunikasi, karena banyak sekali kasus keamanan informasi yang terjadi karena cara berkomunikasi yang tidak aman. Keamanan informasi bukan hanya bergantung kepada teknologi yang menjaga informasi tersebut saja, tetapi juga menyangkut pengguna teknologi tersebut yang lebih sering dikategorikan sebagai faktor manusia dalam keamanan informasi. Berdasarkan penelitian oleh Verizon, salah satu perusahaan telekomunikasi di Amerika yang dilakukan pada tahun 2010, 28% persen kebocoran data terjadi karena *social attack* yang memanfaatkan faktor manusia ini [1].

Keamanan informasi biasanya dapat dilihat dalam 3 aspek yaitu sebagai berikut.

a. *Confidentiality*

   Aspek ini merupakan aspek kerahasiaan dari informasi, yang dapat diartikan bahwa yang memiliki hak akses terkait informasi tersebut hanyalah orang-orang yang berhak saja. Informasi harus dijaga dengan baik agar tidak dapat diakses oleh orang atau pihak yang tidak berhak.

b. *Integrity*

   Aspek ini merupakan aspek keaslian dari informasi, yang dapat diartikan bahwa informasi lengkap dan tidak berubah dari kondisi aslinya. Informasi harus dijaga agar tidak dirubah atau dimodifikasi oleh orang atau pihak yang tidak berhak sehingga tetap utuh dan akurat.

c. *Availability*

   Aspek ini merupakan aspek ketersediaan dari informasi, yang dapat diartikan bahwa informasi harus dapat diakses secara mudah dalam waktu yang tepat oleh orang yang memiliki akses terhadap informasi tersebut.

Berdasarkan ketiga aspek tersebut, aspek yang vital adalah aspek *confidentiality*. Hal ini terjadi karena dalam lingkungan kerja *Work From Home*, banyak orang yang tidak memiliki

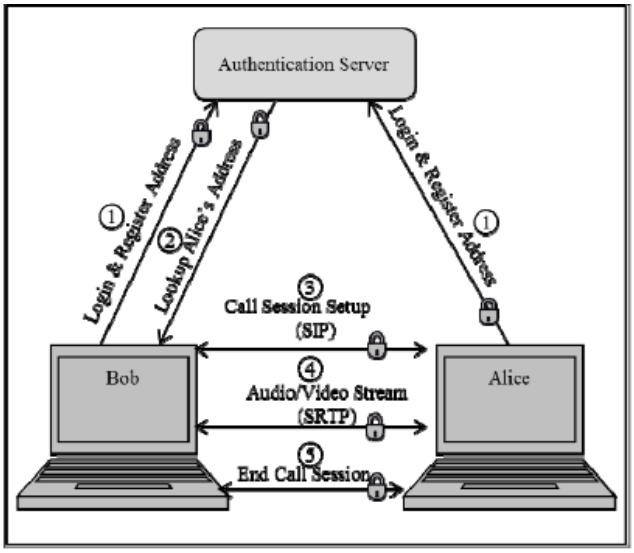
kesadaran dan pengetahuan terkait teknologi dan informasi. Terkait teknologi, ada banyak orang yang sebelumnya tidak terlalu fasih dalam teknologi, terutama generasi X yang tentunya tidak terpapar teknologi sebanyak generasi-generasi lainnya seperti milenial ataupun generasi Z.

Tidak jarang dilakukan rapat ataupun pertemuan yang membahas hal-hal vital dengan media konferensi video yang dapat dengan mudah dimasuki oleh siapapun secara online, tanpa perlu menggunakan verifikasi apapun. Hal ini tentunya membuat informasi yang ada di dalam pertemuan itu menjadi sangat terancam oleh pihak-pihak yang tidak berhak terhadap informasi tersebut.

Arsitektur Aplikasi Konferensi Video

Aplikasi konferensi video sendiri bukan merupakan teknologi yang sangat baru. Konsep dari pertemuan secara jarak jauh sudah ada sejak sekitar tahun 1870, sebagai perpanjangan dari teknologi telepon. Teknologi video call dikembangkan secara resmi oleh Bell Labs and John Logie Baird dari perusahaan AT&T pada tahun 1927 dan menjadi layanan konferensi video yang sudah sangat mirip dengan teknologi sekarang pada tahun 1970 [2].

Untuk sekarang, aplikasi konferensi video sudah menjadi aplikasi yang dapat dengan mudah digunakan dan disediakan oleh berbagai perusahaan. Secara garis besar alur dari aplikasi konferensi video dapat dilihat pada gambar berikut.



Gambar 1 Alur Aplikasi Konferensi Video

Pertama, perlu dilakukan registrasi pengguna yang akan menggunakan layanan konferensi video kepada server. Lalu salah satu pengguna akan melakukan *lookup* terhadap pengguna lainnya untuk kemudian melakukan sebuah inisiasi misalkan dengan *session initiation protocol*. Setelah kedua belah pihak melakukan inisiasi seperti persetujuan terhadap format media, *video codecs*, algoritma enkripsi, *port* yang digunakan, dan beberapa parameter teknis lainnya, maka akan dimulai pembagian audio dan juga video menggunakan protokol media seperti *session real time protocol* [3]. Lalu jika sudah selesai maka sesi layanan tersebut akan diakhiri.

Beberapa poin penting yang harus dilihat pada interaksi antara kedua belah pengguna adalah sebagai berikut [2].

a. Identitas pengguna

   Identitas yang dipakai oleh pengguna untuk mendaftarkan dirinya kepada server penyedia layanan konferensi video. Identitas ini biasanya berupa nama, alamat email, tempat, platform yang digunakan, serta informasi-informasi lainnya yang juga bervariasi tergantung penyedia layanan.

b. Audio dan Video

   Merupakan inti dari interaksi yang dilakukan oleh pengguna. Komunikasi tersebut dapat dibagi menjadi dua secara garis besar yaitu melalui suara (audio) dan juga gambar (video). Tergantung dari konteks interaksi yang dilakukan, informasi bisa saja sangat penting dan sensitif.

c. Kode media

   Kode yang digunakan untuk memproses media tersebut, berupa proses enkripsi deskripsi, proses *encoding decoding*, serta proses *rendering* audio dan video secara *real-time.*

d. Peraturan

   Peraturan-peraturan yang ada dalam interaksi melalui konferensi video tersebut. Peraturan tersebut dibuat untuk membatasi informasi agar tetap aman, misalkan peraturan tentang riwayat layanan, tentang larangan untuk melakukan rekaman, dan lain-lain.

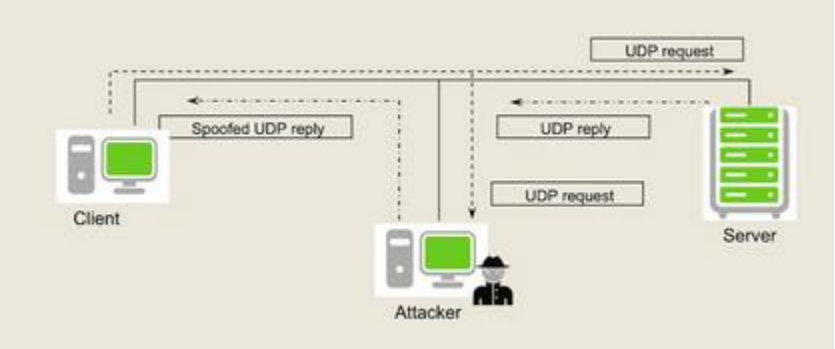
Keamanan Aplikasi Zoom

Zoom adalah salah satu aplikasi konferensi video yang sekarang sangat populer. Hal ini disebabkan karena penggunaannya yang mudah dan dianggap sangat efektif untuk berkomunikasi. Konsep dari aplikasi ini sendiri sudah dipikirkan oleh Eric Yuan sejak 1987, tetapi baru direalisasikan pada tahun 2011 dan rilis pada tahun 2012 dengan kapabilitas untuk menampung sampai dengan 15 orang, kuantitas yang besar saat itu.

Aplikasi zoom pun melonjak dalam angka pemakaiannya sejak terjadi pandemi COVID-19, tetapi ada banyak sekali kritik yang dilancarkan kepada Zoom terkait keamanan dan juga privasi data yang dimiliki olehnya. Zoom juga tidak pernah memberitahu arsitektur sistem dan aplikasi miliknya (*closed source*) sehingga sulit untuk dinilai oleh para peneliti secara jelas. Berdasarkan pernyataan resmi dari Zoom, beberapa teknologi yang dipakai olehnya beserta masalah yang berpotensi terhadap teknologi tersebut adalah sebagai berikut.

a. Unencrypted UDP Messages

   Zoom memiliki enkripsi yang tidak terlalu jelas, terbukti dari kasus pada tahun 2018 dimana terdapat celah keamanan dimana pada sesi enkripsi yang terjadi saat konferensi video, pesan UDP(*User Datagram Protocol*) yang tidak terenkripsi dapat diterima oleh pengguna. Sehingga penyerang dapat melakukan *spoofing* jika mengetahui *IP address* dari target atau *IP address* yang dipakai oleh server Zoom. Penyerang juga membutuhkan *id* pertemuan dari target, tetapi hal tersebut dapat dengan mudah diketahui dengan cara *brute-force* [4]. Setelah target menerima UDP yang sudah dimodifikasi oleh penyerang, maka penyerang dapat menggunakan akses dari Zoom untuk melakukan pembajakan terhadap target, seperti membajak *platform* target, membajak pesan, dan juga melakukan kekacauan yang disengaja dengan mengeluarkan orang yang sedang berpartisipasi di dalam konferensi tersebut.

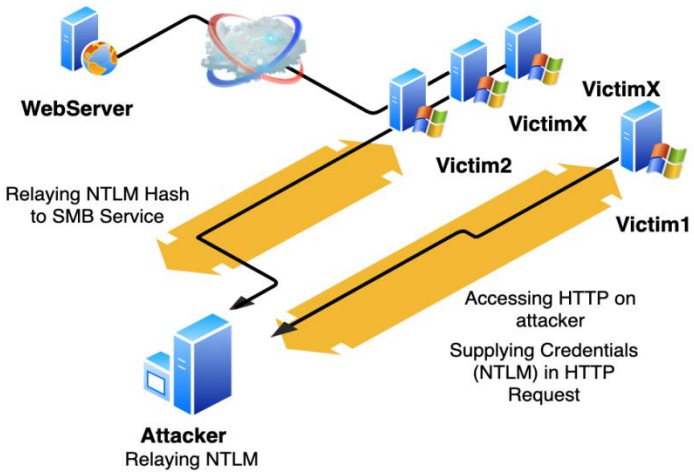


Gambar 2 Ilustrasi *UDP Spoofing*

b. Universal Naming Convention Bug

Zoom pada sistem operasi windows memiliki bug dimana pada layanan *chat* yang disediakan dapat dikirim sebuah *universal naming convention string* yang menjadi sebuah link yang dapat diklik. Penyerang memanfaatkan hal ini untuk membuat link tersebut yang bila ditekan oleh target dapat mengirimkan *username* windows dan juga Net-NTLM-v2 hash milik target kepada penyerang [5].

Penyerang dapat memanfaatkan kredensial dari target tersebut untuk melancarkan serangan *SMBRelay attacks* seperti pada gambar berikut.



Gambar 3 Ilustrasi *SMBRelay attacks*

Dapat dilihat bahwa penyerang mendapatkan kredensial dari target melalui sebuah *HTTP request*, lalu dapat menggunakannya untuk melakukan akses kepada sumber daya bersama yang tersedia pada windows, seperti server *outlook* ataupun media

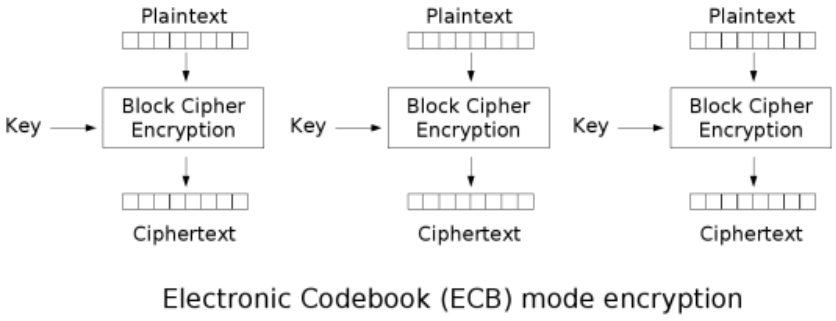
penyimpanan. Hal ini dapat dilakukan karena hash yang didapatkan tidak perlu dikonversi menjadi kata sandi normal, tetapi dapat langsung digunakan untuk melakukan otorisasi peran dari pengguna. Sampai April 2020 masih ada beberapa kasus yang terjadi dan pihak resmi Zoom mengatakan bahwa *bug* ini akan segera diperbaiki.

c. Call Routing yang tidak sesuai dengan wilayah

Proses konferensi video yang terjadi tentunya harus terkoneksi dengan *datacenter* yang dimiliki oleh penyedia layanan, dan untuk meningkatkan reliability dari layanan tersebut datacenter sebaiknya berada di dekat pengguna. Zoom sendiri memiliki fitur *geofencing* yang berarti pengguna akan terkoneksi pada *datacenter* yang berada paling dekat dengannya, dan jika terjadi masalah jaringan maka akan melakukan koneksi ke *datacenter* lain yang dekat. Namun beberapa kasus yang terjadi adalah rute dari konferensi video yang dilakukan di Amerika dan Eropa melalui Cina. Hal ini tentunya cukup mengkhawatirkan karena Cina memiliki otoritas yang independen salah satunya terhadap peraturan terkait data, sehingga ada potensi bahwa data pada *datacenter* yang ada di Cina tersebut dapat didekripsi dan isi dari konferensi dapat diketahui dengan mudah.

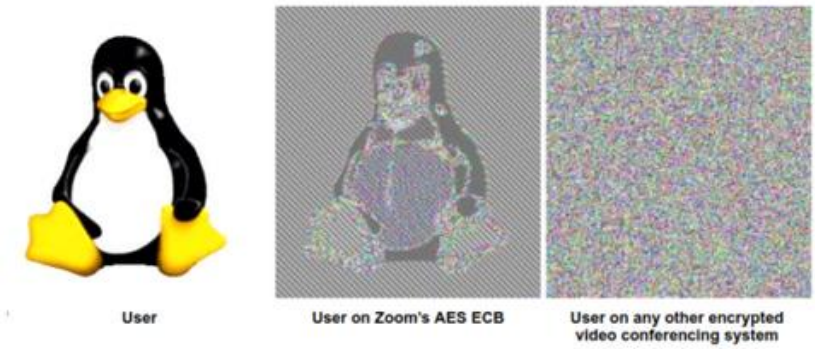
d. Enkripsi AES-128

Zoom mengatakan bahwa pihak mereka menyediakan layanan konferensi video dengan enkripsi AES-256, tetapi setelah diteliti lebih lanjut Zoom menggunakan enkripsi AES-128 dengan mode ECB yang telah diketahui memiliki banyak kelemahan dan ancaman keamanan [4].



Gambar 4 Cara Kerja Enkripsi ECB

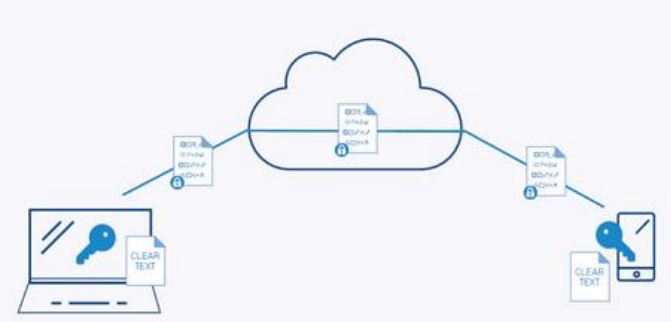
Pada mode tersebut, blok *plaintext* yang identikal akan menghasilkan blok *ciphertext* yang identikal pula, sehingga dapat terlihat suatu pola yang dapat dengan mudah dikenali oleh penyerang meskipun tidak menggunakan formula matematis apapun untuk melakukan dekripsi terhadap blok tersebut. Secara sederhana *ECB mode* dapat dijelaskan pada gambar berikut, dimana konferensi video yang menggunakan enkripsi dari zoom dapat terlihat dengan jelas [6].



Gambar 5 Ilustrasi Enkripsi AES ECB

e. Enkripsi *end-to-end* yang tidak sesuai

Dalam layanan konferensi video, jika pengguna mencoba melihat pemberitahuan dari aplikasi Zoom, maka akan tampil tulisan yang mengatakan bahwa layanan ini dienkripsi secara end to end. Enkripsi *end to end* merupakan salah satu enkripsi yang sangat aman karena hanya pengguna saja yang dapat melakukan dekripsi dan mengetahui isi dari pesan konferensi video tersebut.



Gambar 6 Ilustrasi Enkripsi *end to end*

Seperti terlihat pada gambar, bahwa kunci hanya dimiliki oleh pengguna saja [7]. Server yang menjadi penyedia layanan memiliki pesan yang sudah dienkripsi, tetapi tidak memiliki kunci untuk melakukan dekripsi untuk mengetahui isi pesan tersebut.

Tetapi setelah diteliti lebih lanjut, Zoom ternyata menggunakan *transport encryption* yang terdiri dari TCP dan UDP, sama seperti enkripsi yang terjadi jika mengakses *website* dengan *http*. Hal ini berarti Zoom dapat melakukan enkripsi dan melihat seluruh pesan pada konferensi video pengguna [6].

Berdasarkan beberapa ancaman keamanan diatas yang sudah dijelaskan, dapat diketahui bahwa Zoom bukanlah merupakan pilihan aplikasi konferensi video yang memiliki struktur keamanan ataupun privasi data yang baik untuk penggunanya. Sampai tanggal 29 April 2020 pun Zoom masih dilancarkan berbagai kritik dan tuntutan terkait celah-celah keamanan yang dimilikinya, serta berbagai teknologi yang ternyata berbeda dengan pernyataan resmi dari mereka. Adapun beberapa aplikasi penyedia layanan konferensi video yang dapat digunakan sebagai alternatif Zoom, dengan keamanan yang lebih jelas dan terbukti adalah sebagai berikut.

a. Signal

   Signal merupakan salah satu aplikasi penyedia layanan konferensi video yang mendukung enkripsi *end to end* dengan *Signal Protocol* yang open source dan sudah dibuktikan oleh para ahli. Namun fungsionalitas dari Signal tidak terlalu baik, dengan fitur yang terbatas pula.

b. Jitsi

   Jitsi merupakan aplikasi yang baru saja masuk ke pasar dan sudah mendapat banyak atensi dari masyarakat. Jitsi tidak mendukung enkripsi *end to end*, tetapi terdapat fitur dimana perusahaan dapat melakukan *self-hosting*. Jitsi juga merupakan aplikasi yang tidak berbayar sehingga mudah untuk didapatkan oleh semua orang.

c. Cisco Webex

   Webex merupakan salah satu aplikasi yang juga cukup populer dan memiliki kredibilitas tinggi karena layanan ini disediakan oleh Cisco. Webex juga menyediakan enkripsi *end to end* dengan pembayaran yang bervariasi sesuai dengan kebutuhan.

Penutup

Di tengah masa pandemi COVID-19, tentunya diperlukan sebuah fasilitas yang dapat mengganti pertemuan-pertemuan secara fisik. Salah satu pilihannya adalah konferensi video, dimana Zoom menjadi aplikasi yang sangat populer untuk digunakan karena menyediakan berbagai fungsionalitas yang membuatnya mudah dan efektif untuk dipakai. Namun dibalik fungsionalitas tersebut, Zoom juga memiliki berbagai masalah keamanan seperti enkripsi, *bug*, *routing*, dan lain-lain yang menimbulkan celah keamanan yang sangat serius terutama untuk privasi data penggunanya.

Zoom tetap merupakan salah satu aplikasi yang sangat baik untuk layanan konferensi video, tetapi untuk kebutuhan sehari-hari saja. Untuk kebutuhan komunikasi yang membicarakan informasi sensitif ada baiknya menggunakan aplikasi serupa yang menyediakan layanan konferensi video tetapi sudah terbukti lebih aman. Dalam penggunaannya pun para pengguna harus tetap menjaga diri dan menyadari bahaya keamanan yang mungkin dapat dialami misalkan dari link pada group chat, dari pertemuan tanpa kata sandi, dan lain-lain agar keamanan informasi dari pengguna dapat terjaga dengan baik khususnya di lingkungan kerja *Work From Home* ini yang membutuhkan banyak komunikasi secara daring.

Referensi

[1] B. M. Bowen, R. Devarajan and S. Stolfo, "Measuring the human factor of cyber security," *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, Waltham, MA, 2011, pp. 230-235.

[2] R. Lal and P. M. Pappachan, "An architecture methodology for secure video conferencing," *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, Waltham, MA, 2013, pp. 460-466.

[3] C. Du, H. Yin, C. Lin and Y. Hu, "VCNF: A Secure Video Conferencing System Based on P2P Technology," *2008 10th IEEE International Conference on High Performance Computing and Communications*, Dalian, 2008, pp. 463-469.

[4] M. K. Mishra, S. Mukhopadhyay and G. P. Biswas, "Architecture and secure implementation for video conferencing technique," *Proceedings of the 2015 Third International Conference on Computer, Communication, Control and Information Technology (C3IT)*, Hooghly, 2015, pp. 1-6.

[5] C. Lv, M. Ma, H. Li and J. Ma, "A security enhanced authentication and key distribution protocol for wireless networks," *2010 IEEE Globecom Workshops*, Miami, FL, 2010, pp. 1571-1575.

[6] M. Vaidehi and B. J. Rabi, "Design and analysis of AES-CBC mode for high security applications," *Second International Conference on Current Trends In Engineering and Technology - ICCTET 2014*, Coimbatore, 2014, pp. 499-502.

[7] K. Rohloff, D. B. Cousins and D. Sumorok, "Scalable, Practical VoIP Teleconferencing With End-to-End Homomorphic Encryption," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1031-1041, May 2017.