Analisis Keamanan pada Aplikasi Video Berbasis Ponsel dengan Implementasi *Naive Advanced Encryption Standard* (AES)

Zalikha Adiera Gambetta
18217027
Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
zalikhagambetta@gmail.com

Abstrak

Aplikasi video berbasis ponsel membutuhkan keamanan yang tinggi untuk mengamankan konten serta identitas dari penggunanya. Salah satu cara atau metode untuk meningkatkan keamanan tersebut yaitu dengan menggunakan *Advanced Encryption Standard* (AES). AES merupakan algoritma kriptografi yang disetujui oleh Federal Information Processing Standard (FIPS) untuk melakukan enkripsi dan dekripsi data. Ditengah pandemi yang menyebabkan para pekerja dan pelajar harus melakukan aktivitasnya di rumah menyebabkan peningkatan dari penggunaan aplikasi video dan digunakan dari ponsel. Tanpa sadar, terdapat banyak ancaman dari penggunaan aplikasi ini karena dapat mengganggu kelangsungan penggunaan aplikasi. Selain itu, dengan kebutuhan end-to-end enkripsi data, diharapkan dengan hasil analisis penggunaan AES, dapat memberikan informasi lebih kepada penggunanya. Pada makalah ini akan dibahas mengenai bagaimana penggunaan AES dapat meningkatkan keamanan dari aplikasi video berbasis ponsel yang akan didasari oleh hasil analisis dari berbagai penelitian serta dampak yang didapatkan oleh ponsel dengan digunakannya AES sebagai metode enkripsi dan dekripsi di aplikasi. Dijelaskan pula gambaran kelebihan dari AES dibandingkan dengan algoritma lainnya.

Kata Kunci: *Advanced Encryption Standard (AES), enkripsi, dekripsi, aplikasi video berbasis ponsel*

I. Pendahuluan

Penggunaan ponsel pintar semakin meningkat setiap tahunnya dan diperkirakan pada 2020, di Indonesia mencapai 81,87 juta pengguna [1]. Dengan perkembangan teknologi yang ada, hal tersebut mendukung perubahan serta perkembangan dari ponsel pintar dan mendukung kebutuhan penggunanya dari sisi multimedia dan berkomunikasi jarak jauh. Hal tersebut digambarkan dengan banyaknya aplikasi multimedia yang digunakan secara terus menerus yaitu dalam mengirim dan menerima video, konferensi video, dan sebagainya [2]. Dengan maraknya aplikasi *video messaging*, hal tersebut meningkatkan dampak multimedia kepada kehidupan kita sehari-hari.

Terutama dengan adanya pandemi yang terjadi, mengakibatkan para pekerja dan pelajar harus dirumahkan dan segala jenis pekerjaan dilakukan secara *online*. Kegiatan yang sebelumnya merupakan tatap muka, digantikan dengan cara berkomunikasi secara online dengan teks, suara, video, maupun gambar. Dengan meningkatnya penggunaan aplikasi tersebut, keamanan akan privasi dari masing-masing individu menjadi permasalahan utama yang diperhatikan oleh para penggunanya. Kebutuhan berkomunikasi *end-to-end* menjadi tantangan utama dari para penyedia aplikasi multimedia untuk memberikan rasa aman kepada penggunanya dan meningkatkan kepercayaan terhadap aplikasi yang digunakan.

Untuk kebutuhan mentransmisikan data dalam sebuah *streaming video*, dibutuhkan transmisi data yang aman dan dapat melindungi data sensitif yang terdapat didalamnya terutama data-data seperti identitas diri. Selain streaming video, pada *video conferencing*, tak hanya dibutuhkan keamanan pada identitas namun juga dibutuhkan video secara *real-time*. Dengan maraknya aplikasi *streaming video* serta *video conferencing* berbasis ponsel pintar, para penggunanya tidak menyadari bahwa terdapat ancaman yang serius. Namun, terdapat berbagai teknik untuk mengamankan data penggunanya salah satu diantaranya yaitu menggunakan teknik enkripsi.

Berbagai macam teknik enkripsi yang ada untuk transmisi data melalui ponsel pintar, masih terdapat tantangan lain yang muncul yaitu mengenai hidup baterai yang

terbatas. Karena, dengan menggunakan metode enkripsi terutama enkripsi konvensional yang kuat seperti *Advanced Encryption Standard* atau Standar Enkripsi Lanjutan (AES) biasanya meningkatkan overhead komputasi ketika diterapkan ke seluruh data dalam *streaming* video secara *real-time* [2]. Berbagai macam AES yang memiliki kelebihannya masing-masing seperti AES-128 dan AES-256 akan menjadi fokus bahasan pada makalah ini.

Dengan permasalahan terhadap keamanan data pengguna yang terus menerus ada pada aplikasi video berbasis ponsel, pada makalah ini akan dibahas mengenai bagaimana penggunaan *Advanced Encryption Standard* (AES) dapat meningkatkan keamanan data pengguna serta dampak dari enkripsi tersebut terhadap ponsel pintar. Dilakukan pula analisis perbandingan antara algoritma enkripsi lain selain AES untuk memberikan gambaran atas kelebihan dari AES sebagai metode keamanan yang sesuai untuk aplikasi video berbasis ponsel. Diharapkannya dengan analisis tentang enkripsi pada aplikasi video dapat meningkatkan rasa aman untuk pengguna aplikasi video berbasis ponsel.

II. Studi Terkait

A. Video Encryption

Berdasarkan beberapa penelitian, dalam melakukan enkripsi terhadap video dibagi menjadi beberapa klasifikasi. Salah satu klasifikasinya yaitu pendekatan yang digunakan untuk melakukan enkripsi. Berikut merupakan 2 jenis pendekatan yang dapat digunakan untuk melakukan enkripsi pada video [8].

1. *Full Encryption*

   Algoritma dalam melakukan enkripsi video dilakukan kepada seluruh bitstream video (yang terkompresi maupun yang tidak terkompresi). Biasanya, algoritma ini disebut dengan *naive encryption*. Pendekatan *naive* adalah jenis pendekatan enkripsi penuh dimana menggunakan cryptosystem konvensional untuk melakukan enkripsi.

2. *Selective Encryption*

   Pendekatan enkripsi selektif dilakukan dengan melakukan enkripsi hanya pada bit tertentu yang dipilih dengan hati-hati dari bitstream video (yang telah terkompresi atau tidak terkompresi) dan membiarkan sisa bit tidak terenkripsi. Bahkan lebih umum, seseorang dapat mendefinisikan enkripsi variabel menjadi pendekatan di mana tingkat keamanan enkripsi yang berbeda diterapkan pada bit yang berbeda dari input. Enkripsi selektif (juga disebut enkripsi parsial) dapat dilihat sebagai subkategori enkripsi variabel. Jenis khusus dari pendekatan enkripsi selektif di mana bit dipilih berdasarkan informasi spasial disebut sebagai enkripsi selektif spasial. Misalnya, orang dapat memilih untuk mengenkripsi hanya wajah orang yang muncul dalam urutan video.

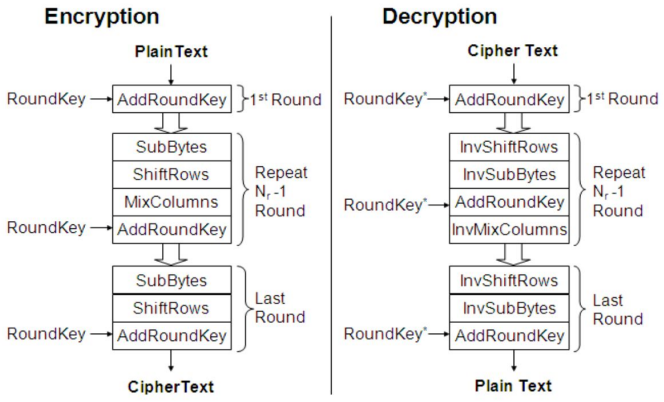
B. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) merupakan algoritma kriptografi yang disetujui oleh Federal Information Processing Standard (FIPS) dan dapat digunakan untuk melindungi data elektronik. Algoritma yang digunakan pada AES merupakan cipher blok simetris yang dapat mengenkripsi dan mendekripsi informasi [3]. Standar ini merupakan hasil spesifikasi dari algoritma Rijndael dan dapat memproses blok data yang berisikan 128 bit menggunakan kunci cipher dengan panjang atau ukuran 128, 192, dan 256 bit [3]. Ukuran dari blok dan kunci tersebut akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi. Kekuatan enkripsi dari cipher dapat ditingkatkan dengan cara meningkatkan jumlah putaran yang dilakukan dalam memproses data. Standar AES menentukan bahwa jumlah putaran ditentukan oleh panjang dari kunci sandi yaitu terdapat pada tabel berikut [4].

Tabel 1: Jumlah putaran dari masing-masing jenis kunci AES

Panjang Kunci	Jumlah Putaran (Nr)
AES-128	10
AES-192	12
AES-256	14

Proses enkripsi AES memiliki 4 tahapan transformasi byte yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Berikut merupakan gambaran dari proses enkripsi dan dekripsi menggunakan metode AES [5].



Gambar 1: Proses dekripsi dan enkripsi menggunakan AES

Proses enkripsi maupun dekripsi diawali dengan AddRoundKey yaitu setiap byte tahapan yang ada dikombinasikan dengan kunci bulat yang dimana setiap kunci putaran tersebut diturunkan dari *cipher key* dengan jadwal kunci. Untuk tahap enkripsi, dilanjutkan dengan SubBytes yang merupakan langkah substitusi non-linear. Setiap byte diganti dengan nilai lain yang terdapat atau sesuai dengan tabel pencarian. ShiftRows merupakan langkah transposisi untuk setiap basis tahapan digeser secara beberapa kali sejumlah langkah yang ada. Kemudian, MixColumns merupakan operasi pencampuran atau penggabungan

dan bekerja pada kolom dari tahapan yang dilakukan. Pada proses dekripsi, dilakukan kebalikan dari proses enkripsi untuk mengembalikan data yang telah diubah ke bentuk *cipher* menjadi data awal yang dikirimkan.

Dengan berbagai jenis kunci cipher, dibutuhkan untuk menganalisis perbedaan dari AES-128 dan AES-256 sebelum menentukan algoritma enkripsi manakah yang dapat meningkatkan keamanan data pengguna pada aplikasi video berbasis ponsel. Berdasarkan beberapa penelitian, dihasilkan hasil analisis perbandingan kedua jenis kunci cipher sebagai berikut [9]. Algoritma AES-128 akan digunakan masukkan dengan ukuran yang tetap yaitu 128 bit yang disebut dengan data blocks. Sedangkan algoritma AES-256 melakukan enkripsi dengan kunci rahasia 256 bit dengan ukuran *plain text* deskripsinya sebesar 16 bytes.

III. Pembahasan

A. Meningkatkan keamanan data pengguna pada aplikasi video berbasis ponsel dengan AES

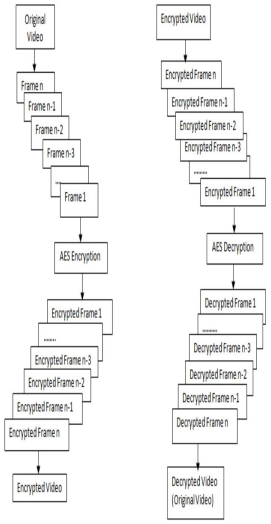
Pada aplikasi video berbasis ponsel, terdapat bermacam-macam aplikasi yang fungsi berbeda-beda dari *live streaming*, *video conferencing*, dan sebagainya. Pada aplikasi yang berfungsi hanya untuk live streaming, penggunaan AES-128 sudah cukup untuk mengamankan kontennya [10]. Tetapi, jika AES-128 tidak didukung dengan *secure key exchange protocol*, apabila seseorang ingin meretas aplikasi tersebut dan telah mendapatkan kuncinya, maka sangat mudah baginya untuk masuk ke aplikasi live streaming tersebut [10].

Pada AES-256, nilai 256 menunjukkan ukuran dari kunci yang menyatakan banyaknya kombinasi kunci yang menghasilkan semakin sulit untuk diretas ataupun ditebak. Akan terdapat 2256 kombinasi yang berbeda untuk meretas pesan yang di enkripsi yang hingga saat ini apabila ingin diretas membutuhkan 50 *supercomputer* yang belum tersedia di pasaran untuk memeriksa hingga 1018 kunci AES per detiknya [9]. Selain itu, dalam

penggunaannya AES-259 akan terdapat pada Transport Layer Security yang berfungsi untuk mengamankan *socket layer*.

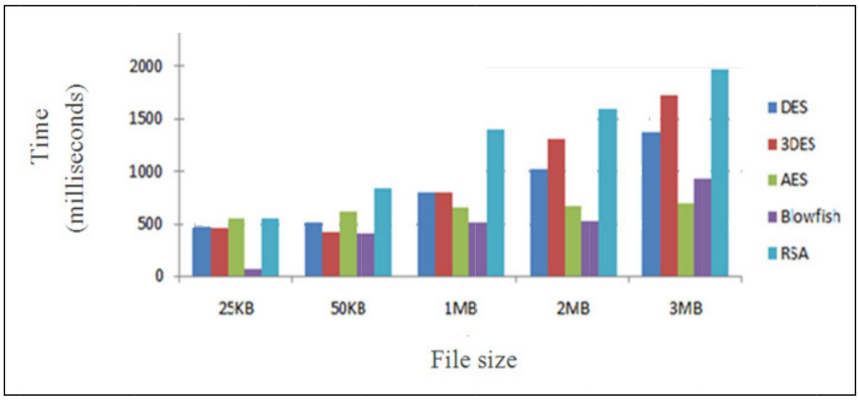
Saat ini, AES-256 merupakan metode enkripsi yang paling baik dibandingkan algoritma AES-128 dan AES-192. Pada teknologi masa kini pun AES-256 banyak ditemukan dan menjadi landasan dari metode algoritma enkripsi modern, protokol, dan teknologi. Berbagai aplikasi salah satunya yaitu Skype, yang memberikan fitur *peer-to-peer video call* menggunakan AES 256. Saat ini skype telah menggunakan end-to-end encryption di setiap sesi yang akan menghasilkan *session key* yang berbeda-beda.

Dengan ini, identitas seseorang akan menjadi lebih aman dan tingkat kepercayaan akan aplikasi video tersebut akan meningkat. Meskipun AES-256 telah banyak digunakan di berbagai aplikasi video berbasis ponsel dan mengaplikasikan *end-to-end encryption*, masih terdapat beberapa aplikasi yang belum mempraktekkannya seperti Zoom. Pada aplikasi Zoom masih digunakan AES-128 dengan mode ECB (*Electronic Code Book*) dan tidak dilakukan enkripsi secara *end-to-end*. Oleh karena itu, sangat rawan untuk aplikasi tersebut karena para peretas dapat dengan mudah masuk ke server dan mengganggu para penggunanya dengan ikut masuk ke dalam meeting atau ruangan di Zoom [11]. Berikut merupakan proses enkripsi video dengan AES-256 [8].

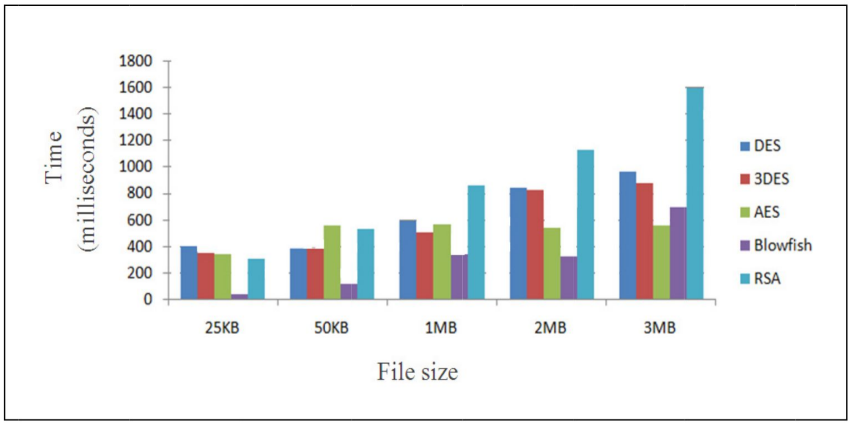


Gambar 2: Proses enkripsi dan dekripsi video dengan AES

Dengan tingkat keamanan yang tinggi, waktu yang dibutuhkan untuk enkripsi dan dekripsi file diperhatikan pula. Berdasarkan hasil penelitian [14], dapat dilihat bahwa waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi menggunakan AES (128, 192, 256) cukup singkat dibandingkan dengan algoritma enkripsi lainnya.



Gambar 3: Hasil perbandingan berbagai algoritma untuk waktu Enkripsi



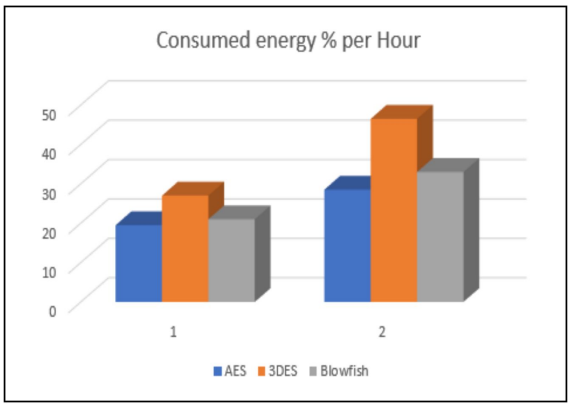
Gambar 4: Hasil perbandingan berbagai algoritma untuk waktu Dekripsi

Pada grafik hasil penelitian [14], ketika AES dibandingkan dengan 4 jenis algoritma enkripsi lainnya, semakin besar ukuran dari file yang dienkripsi maupun didekripsi waktu yang dibutuhkan cukup singkat. Oleh karena itu dapat disimpulkan bahwa AES cukup efisien untuk digunakan sebagai metode enkripsi pada aplikasi video berbasis ponsel.

B. Dampak dari AES di aplikasi video berbasis ponsel terhadap ponsel

Penggunaan algoritma *naive* AES akan berpengaruh terhadap daya baterai ponsel. Pada sebuah penelitian, dilakukan pengujian enkripsi terhadap konsumsi energi ponsel dengan membandingkan berbagai macam jenis algoritma enkripsi video pada ponsel. Algoritma enkripsi *native* melakukan enkripsi seluruh video dengan memperlakukan data video sebagai teks.

Pada penelitian [12], dilakukan eksperimen yang membandingkan 3 algoritma (DES, AES-128, dan BlowFish) konsumsi energi yang digunakan saat melakukan enkripsi video. Eksperimen dilakukan dari 3 ponsel yang berbeda. Masing-masing ponsel akan menonton *streaming video* melalui sebuah aplikasi ponsel yang memiliki fungsi untuk video *streaming* dari *cloud* server. Untuk melihat banyaknya energi yang digunakan, baterai dari ponsel tersebut akan direkam sebelum menonton dan setelah menonton video melalui aplikasi *streaming* tersebut untuk dibandingkan. Energi baterai yang digunakan juga dipengaruhi oleh koneksi *wireless* dan layanan *streaming* video juga. Terdapat 2 jenis ponsel yang digunakan yaitu dengan android 5.0.1 (kapasitas baterai 2600 mAh) dan android 4.4.1 (kapasitas baterai 2000 mAh). Dengan ukuran yang berbeda-beda (dari kunci dan blok algoritma), persentase konsumsi energi setiap jam nya untuk melakukan *streaming* video dengan kualitas tinggi (*high quality video*) yaitu sebagai berikut.



Gambar 5: Hasil perbandingan konsumsi energi pada ponsel dari 3 macam Algoritma enkripsi per jam nya

Dari grafik tersebut, penelitian [12] mengatakan bahwa algoritma AES tidak menggunakan banyak energi saat melakukan video *streaming* untuk kualitas tinggi. Penelitian tersebut juga mengatakan bahwa untuk melakukan enkripsi data yang besar atau banyak, AES sangatlah tepat dan memberikan kinerja yang paling baik dibandingkan dengan algoritma lain. Hal ini menandakan bahwa dengan tingkat keamanan yang tinggi dari algoritma AES dalam melakukan enkripsi data (data tekstual maupun berupa multimedia), ia menggunakan energi yang tidak terlalu besar dan baik untuk diaplikasikan kepada aplikasi video berbasis ponsel untuk meningkatkan keamanan dari konten dan identitas dari penggunanya. Oleh karena itu, para pengguna tidak perlu khawatir akan daya baterai ponselnya akan cepat habis apabila menggunakan aplikasi video berbasis ponsel tersebut.

IV. Kesimpulan

Berdasarkan hasil analisis yang dilakukan terkait keamanan pada aplikasi video berbasis ponsel yang sedang marak digunakan di tengah pandemi, didapatkan hasil bahwa AES merupakan salah satu cara yang paling efektif untuk meningkatkan keamanan dari sebuah aplikasi. Terdapat beberapa macam AES seperti AES-128 dan AES-256 yang memiliki fungsi yang berbeda. Aplikasi *live streaming* sangat sesuai dengan hanya menggunakan AES-128, namun masih terdapat kekurangan yaitu dari sisi

peretasan aplikasi. Karena masih dibutuhkan *secure key protocol* untuk meningkatkan keamanan aplikasi tersebut. Di sisi lain, berdasarkan berbagai penelitian terkait AES-256, didapatkan bahwa AES-256 dapat mengkombinasikan kunci dalam jumlah yang besar sehingga hampir mustahil untuk meretas aplikasi tersebut.

Dengan hasil analisis dari berbagai penelitian pun membuktikan bahwa dengan menggunakan AES untuk melakukan transmisi data yang berukuran besar (seperti video) akan sangat efisien karena waktu yang dibutuhkan untuk mengenkripsi dan mendekripsi data tersebut tergolong paling cepat dibandingkan beberapa algoritma lainnya. Selain itu, dengan hasil analisis penelitian lainnya, didapatkan bahwa penggunaan AES pada aplikasi ponsel menggunakan energi yang tidak terlalu besar dibandingkan dengan metode enkripsi lainnya. Hal ini menjadi salah satu alasan bahwa penggunaan AES terutama AES-256 pada aplikasi video berbasis ponsel merupakan metode yang paling baik untuk meningkatkan keamanan dari sisi konten hingga identitas penggunanya. Sehingga akan meningkatkan kepercayaan dalam menggunakan aplikasi tersebut dari sisi penggunanya.

Referensi

[1] Statista. 2020. *Indonesia Smartphone Users 2011-2022 | Statista*. [online] Available at: <https://www.statista.com/statistics/266729/smartphone-users-in-indonesia/> [Accessed 27 April 2020].

[2] M. A. Saleh, H. Hashim and N. M. Tahir, "A low computational method of secure video streaming in mobile system," 2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), Penang, 2014, pp. 193-197.

[3] NIST: Advanced Encryption Standard. FIPS 197, 2001.

[4] F. Shao, Z. Chang and Y. Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU," 2010 Second International Conference on Communication Software and Networks, Singapore, 2010, pp. 588-590.

[5] T, Prabhakar & Biswal, Birendra & Santhi, Vijaya. (2011). Design and Analysis of Multimedia Communication System. 3rd International Conference on Advanced Computing, ICoAC 2011. 10.1109/ICoAC.2011.6165174.

[6] M S, Rohit & Kunte, Sanjeev. (2014). Selective Video Encryption – A Survey. Recent advances in Computer Engineering. 1. 28-32.

[7] B. Bhat, A. W. Ali and A. Gupta, "DES and AES performance evaluation," International Conference on Computing, Communication & Automation, Noida, 2015, pp. 887-890.

[8] D. M. Dumbere and N. J. Janwe, "Video encryption using AES algorithm," Second International Conference on Current Trends In Engineering and Technology - ICCTET 2014, Coimbatore, 2014, pp. 332-337.

[9] Guy, C., 2020. *A Public Key Encryption Scheme For Detection And Prevention Identification Of Side Channel Attacks To Ensure Security In Cloud Data Centers*. [online] Hdl.handle.net. Available at: <http://hdl.handle.net/10603/249377> [Accessed 28 April 2020].

[10] VdoCipher Blog. 2020. *How AES-128 Encryption For Video Compares To DRM Systems*. [online] Available at: <https://www.vdocipher.com/blog/2018/07/aes-128-encryption-video-drm-secure/> [Accessed 28 April 2020].

[11] Duckett, C., 2020. *Zoom Concedes Custom Encryption Is Substandard As Citizen Lab Pokes Holes In It*. [online] ZDNet. Available at: <https://www.zdnet.com/article/zoom-concedes-custom-encryption-is-sub-standard-as-citizen-lab-pokes-holes-in-it/> [Accessed 28 April 2020].

[12] N. Samet, A. Ben Letaïfa, M. Hamdi and S. Tabbane, "Energy consumption comparison for mobile video streaming encryption algorithm," 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, 2017, pp. 1350-1355.

[13] Toldinas, Jevgenijus & Štuikys, V & Ziberkas, G & Naunikas, D. (1392). Power Awareness Experiment for Crypto Service-Based Algorithms. Elektronika ir Elektrotechnika. 5(101).

[14] Patil, Priyadarshini & Narayankar, Prashant & Narayan, DG & S M, Meena. (2016). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Computer Science. 78. 617-624. 10.1016/j.procs.2016.02.108.