JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 1, Desember 2022, Page 1-8
E-ISSN 2808-005X
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Realisasi Kriptografi Pada Fitur Enkripsi End-To-End Pesan Whatsapp

Sundari Putri Lestari[1], Harris Nur Fadlan[2], Ribka Angelia Purba[3], Indra Gunawan[4]

[1,2,3,4] Program Studi Teknik Informatika, Stikom Tunas Bangsa Pematangsiantar
Email: [1*]sundariputrilestari@gmail.com

Abstrak - Jurnal ini menjelaskan proses yang terjadi dalam pembungkusan data dan algoritma yang digunakan oleh fitur keamanan dalam enkripsi end-to-end WhatsApp. Sistem ini menjamin bahwa pesan yang dikirim antara dua pihak, tidak dapat disadap oleh hacker yang mencegat jalur komunikasi. Dalam komunikasi WhatsApp, pengiriman data bersifat rahasia karena telah melalui proses enkripsi. Enkripsi adalah proses yang dilakukan untuk mengamankan data (yang disebut plaintext) menjadi data tersembunyi (disebut ciphertext). Ciphertext adalah data yang tidak dapat dibaca dengan mudah.

Kata kunci: Enkripsi Ujung ke Ujung, Serangan Man-In-The-Middle, Malware

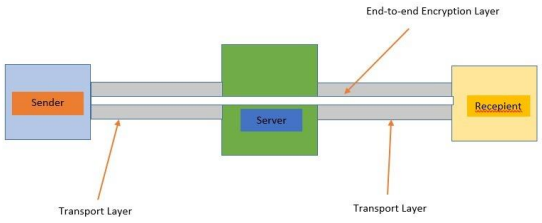
Abstract - This journal explains the process that occurs in data wrapping and the algorithm used by the security features in WhatsApp end-to-end encryption. This system guarantees that messages sent between two parties, cannot be intercepted by hackers who intercept the communication lines. In WhatsApp communication, sending data is confidential because it has gone through an encryption process. Encryption is a process carried out to secure a data (which is called plaintext) into hidden data (called ciphertext). Ciphertext is data that cannot be read easily.

Keywords: End-To-End Encryption, Man-In-The-Middle Attack, Malware

1. PENDAHULUAN

Pencurian data saat ini marak terjadi terutama di rana media sosial, misalnya pada Instagram, facebook, dan whatsapp dan sebagainya. Pengguna harus lebih waspada dalam menggunakan media-media yang menyimpan data-data penting seperti data diri, foto ktp atau apapun yang menyangkut data pribadi lainnya. Oleh sebab itu kerahasiaan data sangat diperlukan saat ini, pengembangan pengamanan yang ketat terus dikembangkan untuk mencegah kebocoran-kebocoran data pribadi[1].

Jurnal ini akan membahas fitur keamanan dari aplikasi chating berbasis android OS yaitu Whatsapp dengan fitur *end-to-end Encryption*. Pada dasarnya fitur ini melindungi data pengguna pada saat dikirim dan dibuka pada saat diterima. Untuk mempermudah pemahaman konsep tersebut dapat dilihat pada gambar 1.0 berikut ini :



Gambar 1. Konsep dasar Enkripsi End-to-end[2],[3]

Pada gambar diatas ditunjukkan bahwa fitur enkripsi end-to-end seolah-olah memiliki jalur sendiri untuk berkomunikasi[4],[5]. Tetapi jalur tersebut hanya perumpaan saja dikarenakan jalur tersebut sebagai pembungkusan data pada komunikasi pengguna. Pada jurnal ini akan dijelaskan lebih detail mengenai proses yang terjadi pada pembungkusan data serta algoritma yang dipakai oleh fitur keamanan pada Whatsapp *end-to-end encryption[6]*. Sistem ini menjamin pesan yang dikirim antara dua pihak, tidak dapat diintip oleh orang lain yang mencegat jalur komunikasi. Jalur komunikasi pesan terenkripsi didukung oleh *Transport Layer Security* yang menghubungkan web client dan software web server.

Submitted: **14/11/2022**; Accepted: **30/11/2022**; Published: **10/12/2022**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 1, Desember 2022, Page 1-8
E-ISSN 2808-005X
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Namun, enkripsi biasa saja tidak cukup, itu sebabnya client software melapisi pesan dengan enkripsi sebelum dikirim ke web client. Pesan tersebut hanya bisa dibuka oleh penerima[7],[8].

Salah satu mekanisme untuk meningkatkan keamanan data dalam pesan whatsapp adalah dengan menggunakan teknologi enkripsi. Data-data yang disimpan dalam whatsapp diubah sedemikian rupa sehingga tidak mudah dibaca. Jadi enkripsi adalah proses yang dilakukan untuk mengamankan sebuah data yang disebut plaintext menjadi data yang tersembunyi atau ciphertext. Ciphertext adalah data yang sudah tidak dapat dibaca dengan mudah oleh pengguna. [9] Kriptografi adalah suatu ilmu pengetahuan (atau lebih tepatnya suatu seni) yang mengenkripsi informasi sehingga sepenuhnya terlihat berbeda dari aslinya.

Berdasarkan plaintext, cipher dapat dikategorikan menjadi dua jenis yaitu block cipher dan stream cipher [10]. Block cipher bekerja memproses data secara blok, dimana beberapa karakter/data digabung menjadi satu blok. Setiap satu blok menghasilkan keluaran satu blok juga. Sementara itu stream cipher bekerja memproses masukan karakter/data secara terus menerus dan menghasilkan data pada saat yang bersamaan. Terdapat beberapa cara untuk melakukan enkripsi [11],[12] yaitu: Enkripsi Simetris (*symmetricencryption*) dan Asimetris (*asymmetricencryption*). Algoritma Enkripsi simetris (*symmetricencryption*) ini menggunakan sebuah kunci rahasia yang sama (*privat key*) untuk melakukan proses enkripsi dan deskripsinya[13],[14]. Algoritma yang dipakai ini termasuk ke dalam algoritma kriptografi klasik yang terdiri dari *substitution cipher* dan *transposition cipher*[15].

2. METODE PENELITIAN

Metode yang digunakan pada penelitian ini adalah metode penelitian analisis. Metode ini merupakan penelitian yang bertujuan menganalisis keamanan pesan whatsapp menggunakan enkripsi end-to-end serta mengembangkan teknologi tersebut untuk dapat mencegah terjadinya pencurian data melalui whatsapp.

Untuk mengumpulkan data dan bahan penelitian maka penulis menggunakan Studi Literatur. Studi literatur adalah mencari referensi teori yang relefan untuk kasus atau permasalahan yang ditemukan. Referensi ini banyak ditemukan dari buku, jurnal, artikel, laporan penelitian, dan situs-situs di internet. Keluaran dari studi literatur ini adalah terkoleksinya referensi yang relefan dengan perumusan masalah. Tujuannya adalah untuk memperkuat permasalahan serta sebagai dasar teori dalam melakukan studi dan juga menjadi dasar untuk melakukan desain dari permasalahan yang diteliti

3. HASIL DAN PEMBAHASAN

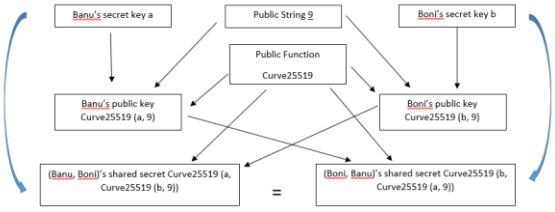
Tipe *Publik Key (Public Key Types*)

a. Identity Key Pair adalah pasangan kunci long-term Curve25519
b. Signed Pre Key adalah pasangan kunci medium-term Curve25519, dibangkitkan saat proses instalasi aplikasi, dan akan berubah dalam waktu tertentu.
c. One-Time Pre Keys adalah barisan pasang kunci Curve25519 yang digunakan hanya satu kali, dibangkitkan saat proses instalasi, dan akan muncul saat dibutuhkan.

Beberapa tipe kunci publik yang digunakan oleh end-to-end encryption pada WA (whatsapp), pasangan kunci yang digunakan berjenis Curve25519. Curve25519 adalah sebuah elliptical curve (ecc) dengan panjang 128 bit yang menggunakan konsep *eliptic curve Diffie-Hellman.* Beberapa yang menjadi pertimbangan dipakainya Curve25519 adalah sisi keamanan yang baik dan beberapa kelebihan dibandingkan dengan algoritma pertukaran kunci yang lain. Pada karya ilmiah Daniel J Bernstein yang berjudul "Curve25519: new Diffie-Hellman speed records" diakui bahwa Curve 25519 memiliki kecepatan komputasi yang baik yang dapat diterapkan pada algoritma kriptografi . Hal ini yang mendasari Whatsapp untuk memakai curve25519 pada fitur end-to-end encryption. Pada konsep dasar Curve25519 tiap pengguna memiliki 32 Byte secret key dan 32 Byte public key. Selain itu, tiap pasangan pengguna memiliki 32 Byte shared key yang digunakan untuk mengotentikasi dan mengenkripsi pesan antar 2 pengguna.. Berikut untuk memperjelas diagram alur pembangkitan *shared key*:

Submitted: **14/11/2022**; Accepted: **30/11/2022**; Published: **10/12/2022**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 1, Desember 2022, Page 1-8
E-ISSN 2808-005X
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin



Gambar 2. Proses pembangkitan shared secret

Pada gambar 2 adalah proses pembangkitan shared secret key yang kemudian akan dijadikan kunci untuk mengenkripsi pesan.
Langkah-langkah pembangkitan adalah sebagai berikut:

1. Kedua user yaitu Banu dan Boni harus sama-sama menentukan *public string* dimana pada gambar *public String* bernilai 9.
2. Kemudian masing-masing Banu dan Boni menentukan *secret key*. Pada gambar *secret key* A untuk Banu dan secret key b untuk Boni. Secret key ini bersifat rahasia.
3. Kemudian Banu dan Bobi membangkitkan kunci public dengan cara memasukan nilai dari *secret key* (a dan b) dan nilai public string (9) ke dalam fungsi Curve25519 yaitu Curve25519 (a, 9) untuk Banu dan Curve25519 (b, 9) untuk Boni.
4. Lalu Banu dan Boni saling bertukar kunci public yang telah dimasukan ke fungsi Curve25519.
5. Terakhir keduanya dapat menghitung dengan cara memasukan *public key* yang didapat dan nilai *secret key* masing-masing kedalam Curve25519. Sebagai contoh Curve25519 (a, Curve25519 (b,9)) untuk shared key Banu dan Boni.

Adapun beberapa kelebihan dari konsep Curve25519:

1. *Extremely High Speed* = Dalam karya ilmiah telah dibuktikan dalam beberapa Personal Computer bahwa Curve25519 memiliki kecepatan yang mampu untuk sebuah proses (*cycles*).
2. *No Time Variability* = Curve25519 telah diriset tahan terhadap *timing attack*, *cache timing attack*, dan *hyperthreading attack*.
3. *Short Secret Key* = Pada Curve25519 memiliki 32 Byte *secret key*
4. *Short Public Key* = Pada Curve25519 memiliki 32 Byte *public key*

3.1 Tipe Kunci Sesi (*Session Key Types*)

a. *Root Key* ialah sebuah nilai dengan panjang 32 Byte digunakan untuk membangkitkan *Chain Keys*.
b. *Chain Key* ialah sebuah nilai dengan panjang 32 Byte digunakan untuk membangkitkan *Message Keys*.
c. *Message Key* ialah sebuah nilai dengan panjang 80 Byte yang digunakan untuk mengenkripsi isi pesan, dari 80 Byte dan 32 Byte yang digunakan sebagai kunci AES-256

3.2 Registrasi Pengguna (*Client Registration*)

Pada waktu awal registrasi, user akan mengirimkan *public Identity Key*, *Signed Pre Key*, dan sejumlah *public One*-Time *Pre Key* ke server software. Server Whatsapp menyimpan *public key* ini beserta identitas dari user tersebut.

3.3 Inisialisasi Pembentukan Sesi

Dalam berkomunikasi dengan pengguna yang lain, pertama user harus menyiapkan sebuah sesi untuk berkomunikasi yang aman. Sesi ini dibentuk hanya satu kali. Jika suatu saat ingin berkomunikasi maka dilakukan kembali dengan user yang sama dan tidak perlu membuat sesi yang baru lagi sampai suatu saat sesi yang telah dibentuk hilang dikarenakan install ulang aplikasi atau perpindahan pengguna ke perangkat yang lainnya.

Submitted: **14/11/2022**; Accepted: **30/11/2022**; Published: **10/12/2022**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 1, Desember 2022, Page 1-8
E-ISSN 2808-005X
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Berikut adalah proses pembentukan sesi :

1. Inisiator adalah user yang pertama kali meminta berkomunikasi dengan user lain. Inisiator meminta *public Identity Key*, *public Signed Key*, dan *single public One-Time Pre Key* milik user lain.
2. Server akan mengembalikan permintaan dengan suatu nilai *public key*. Satu *One-Time Pre Key* yang hanya bisa digunakan satu kali, jadi setelah dikirim dan diterima inisiator maka *One-Time Pre Key* akan terhapus otomatis dari storage server.
3. Inisiator akan menyimpan *Identity Key* milik penerima sebagai $I_{penerima}$, *Signed Pre Key* sebagai $S_{penerimat}$, dan *One-Time Pre Key* sebagai $O_{penerima}$.
4. Lalu inisiator akan membangkitkan sebuah pasangan kunci ephemeral Curve25519 sebagai $E_{initiator}$.
5. Inisiator mengisi Identity Key dengan $I_{initiator}$.
6. Kemudian, inisiator menghitung master secret yaitu master_secret = ECDH($I_{initiator}$, $S_{penerima}$) | | ECDH($E_{initiator}$, $I_{penerima}$) | | ECDH($E_{initiator}$, $S_{penerima}$) | | ECDH($E_{initiator}$, $O_{penerima}$).
7. Inisiator menggunakan HKDF agar membangkitkan *Root Key* dan *Chain keys* dari *master_secret*.

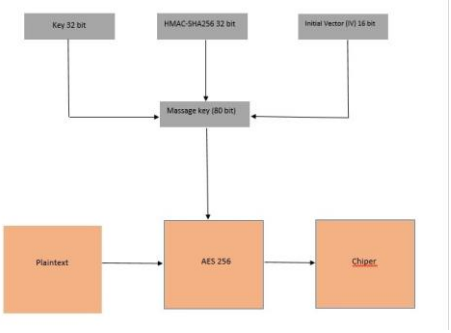
3.4 Pengaturan Sesi Penerimaan (*Receiving Session Setup*)

Setelah dilakukan pembentukan sesi enkripsi, inisiator dapat langsung memulai pengiriman pesan ke penerima, bahkan jika penerima dalam keadaan offline sekalipun sampai direspon oleh penerima. Ketika penerima menerima pesan maka akan menghitung *master_secret* dengan menggunakan *private key* dan *public key* yang terpasang pada header paket informasi yang didapat. Lalu, penerima dapat menghapus *One-Time Pre Key* yang digunakan oleh inisiator..

3.5 Pertukaran Pesan (*Exchanging Messages*)

Dalam berkomunikasi, pertama kali yang dilakukan adalah menyiapkan sesi. Setelah sesi telah terbentuk maka pertukaran pesan dapat dilakukan. Pada Whatsapp pertukaran pesan antar pengguna akan dilindungi dengan *Message Key* yang menggunakan enkripsi AES256 pada mode *Chiper Block Chining* serta menggunakan HMAC-SHA256 sebagai integritas data. *Message Key* akan selalu berbeda pada tiap pesan yang dikirim karena bersifat ephemeral. *Message Key* yang telah mengenkripsi pesan tidak dapat lagi mengenkripsi ulang pesan tersebut.

Berikut adalah blok diagram proses enkripsi pesan, ditunjukkan pada gambar 3 :



Gambar 3. Pertukaran Pesan

Pada gambar 3 ditunjukkan algoritma enkripsi yang digunakan berupa AES-256.Untuk Kunci atau *Message Key* dari AES-256 yang sepanjang 80 Byte terdiri dari 32Byte kunci, 32 Byte HMAC-SHA256, dan 16 Byte iv(*initial vector*). Pada prosesnya pembangkitan *Message key* dapat diperoleh

Submitted: **14/11/2022**; Accepted: **30/11/2022**; Published: **10/12/2022**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 1, Desember 2022, Page 1-8
E-ISSN 2808-005X
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

dari *Chain key*. *Message Key* dibutuhkan setiap waktu oleh inisiator untuk mengenkripsi data. Berikut gambar blok diagram pembentukan *Message*:

Gambar 4. Proses pembangkitan *Message Key*

Berikut cara agar mendapatkan nilai *Message Key* :

1. *Message Key*

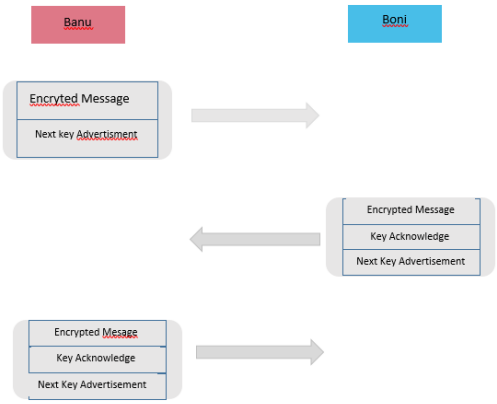
HMAC-SHA256 (Chain Key, 0x01)

2. Dan *Chain key* kemudian diupdate dengan menggunakan proses penghitungan :

Chain Key = HMAC-SHA256 (Chain Key, 0x02)

3.5.1 Advanced Cryptographic Racheting

Chain Key yang dibangkitkan berjumlah 32 Byte yang bersifat "rachets". Metode rachets dibuat oleh *open whisper system* yang digunakan dalam mengatasi masalah pertukaran kunci public enkripsi yang sama pada saat tertentu. Metode ini dapat memastikan kunci public yang dikirimkan berbeda pada tiap pengiriman paket. Fitur ini merupakan protocol keamanan modern yang digunakan untuk mencegah penyerang yang biasa melakukan sniffing jaringan, yang nantinya untuk mencoba melakukan dekripsi karena hanya menggunakan satu kunci saja. Selain itu dengan metode pertukaran kunci singkat, akan menyulitkan bagi penyadap untuk mendapatkan kunci selanjutnya dikarenakan kunci hanya disimpan di memori dan hanya sementara dalam waktu singkat. Berikut gambar yang dapat mengilustrasikan konsep metode "*ephemeral key exchange*".



Gambar 5. Proses *ephemeral key exchange* pada ratchet

Gambar tersebut adalah proses "ephemeral key exhange" yang dilakukan pada saat sesi telah dibangun. Tiga langkah dari gambar tersebut dapat dijelaskan sebagai berikut :

1. Aufa mengirimkan pesan terenkripsi kepada Bobi, dan bersamaan dengan isi dari pesan yang sebenarnya, Aufa juga mengirimkan kunci "advertises" yang digunakan sebagai kunci pada pengiriman pesan berikutnya.
2. Bobi mengirimkan pesan terenkripsi kepada Aufa. Pada saat bersamaan, Bobi juga mengirimkan "*acknowledges*" kunci yang diberikan oleh Aufa, dan mengirimkan kunci Bobi untuk dipakai pada komunikasi berikutnya.

Aufa akan menggunakan kunci *advertised* dan *acknowledged* pada pengiriman pesan berikutnya.

Submitted: **14/11/2022**; Accepted: **30/11/2022**; Published: **10/12/2022**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 1, Desember 2022, Page 1-8
E-ISSN 2808-005X
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

3.6 Konsep Grouping (*Grouping Message*)

Pada beberapa aplikasi chating mempunyai fitur *"grouping"* yang mana fitur ini dapat membuat suatu room yang bisa di isi oleh beberapa orang. Pada prosesnya teknis pengiriman data pada fitur ini terbagi menjadi *server-side* fanout dan *client-side fan out*. Perbedaannya terdapat pada proses pengirimannya. Misalnya *server-side fan-out*, pengirim akan mengirimkan suatu pesan ke dalam suatu grup, didalam pesan tersebut tidak langsung dikirimkan ke seluruh anggota yang ada di dalam grup, melainkan pesan akan dikirim terlebih dahulu ke server. Lalu server yang meneruskan pesan terenkripsi ke dalam grup. *Client-side fan out* mengharuskan pesan yang dikirim akan langsung dikirimkan ke seluruh anggota yang ada didalam grup. Ini akan menyebabkan beban berat yang harus ditanggung oleh pengirim dan menyebabkan proses menjadi lambat karena keterbatasan spesifikasi perangkat itu sendiri.

Berikut adalah proses inisialisasi suatu anggota grup akan mengirim suatu pesan ke group itu:

- Pengirim akan membangkitkan nilai acak sepanjang 32 Byte *Chain Key*.
- Pengirim akan membangkitkan bilangan acak pasangan Curve25519 *Signature Key*.
- Pengirim akan mengkombinasikan 32 Byte *Chain Key* dan *Public key* dari Signature key kedalam pesan *Sender Key*.
- Pengirim akan mengenkripsi *Sender Key* secara pribadi untuk dikirimkan ke setiap anggota grup tersebut.

Setelah proses inisialisasi selesai maka proses selanjutnya pengiriman pesan oleh suatu anggota ke dalam grup adalah :

- Pengirim memperoleh *Message Key* yang berasal dari *Chain Key*, serta *update* dari *Chain Key* sebelumnya.
- Pengirim akan mengenkripsi pesan menggunakan AES256 pada mode CBC.
- Pengirim akan menandai chipertext menggunakan *Signature Key*.
- Pengirim akan mengirim pesan terenkripsi ke server, dan server meneruskan ke seluruh anggota grub.

3.7 Call Setup

Fitur *end-to-end encryption* WA(whatsapp) terdapat pada mode panggilan. Ketika kedua pengguna whatsapp sedang melakukan komunikasi jalur yang dipakai sudah terenkripsi dengan metode SRTP (*Secure Real-Time Transport Protokol*). SRTP khusus didesain untuk pengiriman suara atau video secara langsung. Fitur yang dimiliki oleh protkol ini antara lain menjaga kerahasiaan data (*confidentiality*), Autentikasi pesan, serta perlindungan umpan balik / *replay* dati trafik RTP.

Proses panggilan yang dilakukan pengguna pada whatsapp :

- Inisiator akan membentuk sebuah sesi yang terenkripsi dengan penerima, jika sesi belum terbentuk sebelumnya.
- Inisiator akan membangkitkan nilai acak 32 Byte SRTP *master secret*.
- Inisiator akan mengirim pesan terenkripsi kepada penerima berupa tanda panggilan masuk
- Jika penerima merespon atau menjawab panggilan, SRTP secara otomatis mengenkripsi panggilan tersebut.

4. KESIMPULAN

Pengiriman data yang dilakukan pada komunikasi whatsapp bersifat rahasia karena telah melalui proses enkripsi. Data-data tersebut berupa data rekaman pembicaraan, gambar, video, audio, pesa suara (*voice message*), serta file-file. Fitur *end-to-end* whatsapp berguna dalam pencegahan pihak ketiga (*attacker*)

Submitted: **14/11/2022**; Accepted: **30/11/2022**; Published: **10/12/2022**

dalam mencuri data. Karena data bersifat rahasia (*confidential*). Begitu juga dalam mencegah perubahan data, karena fitur ini juga menjaga keaslian (integritas).

Pada fitur *end-to-end encryption* ini juga memakai metode-metode yang telah teruji dari berbagai sisi. Seperti halnya algoritma yang dipakai untuk enkripsi pesan dan algoritma pertukaran kunci yang dipakai. Hal ini dikarenakan aplikasi whatsapp berbentuk aplikasi mobile dimana memerlukan komputasi se-efisien mungkin agar proses relative cepat.

REFERENSI

[1] R. Kusnadi and M. Jannah, "Penerapan Jaringan Syaraf Tiruan Untuk Memprediksi Jumlah Bagasi Lion Air dan Batik Air di Bandar Udara Kualanamu Dengan Metode Backpropagation," vol. 3, no. 3, pp. 293–302, 2021.

[2] A. Juanda and F. A. Sianturi, "Sistem Pendukung Keputusan Pemilihan Karyawan Tetap pada Trinity Teknologi Nusantara Dengan Metode Moora," JIKOMSI [Jurnal Ilmu Komputer dan Sistem Informasi], vol. 3, no. 3, pp. 277–282, 2021.

[3] S. K. Sari and J. Manurung, "Implementasi Jaringan Syaraf Tiruan Untuk Memprediksi Tingkat Pemahaman Siswa Pada Mata Pelajaran Ujian Akhir Sekolah (UAS) Di SD Mis An Nur Sukamandi Menggunakan Metode Backpropragation," vol. 3, no. 3, pp. 283–292, 2021.

[4] R. P. Fhonna and A. R. Marzuki, "Sistem Informasi Absensi Pegawai Pada Biro Kominfo Kantor Bupati Kabupaten Aceh Utara Berbasis Web," Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI), vol. 3, no. 3, pp. 333–340, 2021.

[5] A. Lestari and B. Sinaga, "Implementasi Metode Backpropagation Memprediksi Tingkat Pemahaman Siswa Pada Mata Pelajaran Pendidikan Agama Islam (PAI) di MTs . S Ummi Lubuk Pakam," Jurnal Ilmu Komputer dan Sistem Informasi, vol. 3, no. 3, pp. 251–276, 2021.

[6] Y. Perwira, "Sistem Pendukung Keputusan Pemilihan Guru Berprestasi di SMK Negeri 1 Pantai Labu Dengan Menggunakan Metode Technique For Order Of Preference By Similarity To Ideal Solution (Topsis)," vol. 3, no. 3, pp. 229–250, 2021.

[7] W. Vrayuda and Y. Perwira, "Penerapan Metode Analytical Hierarchy Process (AHP) Dalam Rekomendasi Subsidi Listrik (Studi Kasus: Desa Pulau Tagor Baru Kec. Galang)," … Komputer dan Sistem Informasi …, vol. 3, no. 3, pp. 202–227, 2021, [Online]. Available: http://ejournal.sisfokomtek.org/index.php/jikom/article/view/117

[8] Mazen Tawfik Mohammed, Alaa Eldin Rohiem and Ali El-moghazy, "Confidentiality Enhancement of Secure Real Time Transport Protocol", Computer Engineering Conference (ICENCO), 2012 8th International, 2014, pp 43-48

[9] WhatsApp Encryption Overview. (2016). Retrieved from Whatsapp official website: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

[10] Advanced Cryptographic Ratcheting. (2016). Retrieved from Open Whisper Systems website: https://whispersystems.org/blog/advanced-ratcheting/

[11] Ruth Nelson, "End-to-End Encryption at the Network Layer", Computer Security Applications Conference, 1989., Fifth Annual, 1989, pp. 28

[12] Vasily Sidorov and Wee Keong Ng, "Transparent Data Encryption for Data-in-Use and Data-at Rest in a Cloud-Based Database-as-a-Service Solution", 2015 IEEE World Congress on Services, 2015, pp. 221-228

[13] Mehdi Asnaashari, 2008, "Method and system for encryption of information stored in an external nonvolatile memory", United States, WO2008127408 A2

[14] Daniel J. Bernstein, 2006, "Curve25519: new Di_e-Hellman speed records"

Submitted: **14/11/2022**; Accepted: **30/11/2022**; Published: **10/12/2022**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 1, Desember 2022, Page 1-8
E-ISSN 2808-005X
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin
[15] Munir, Rinaldi. 2006. Kriptografi. Bandung : Penerbit Informatika (Remove all additional red information like this in your submission script)

Submitted: **14/11/2022**; Accepted: **30/11/2022**; Published: **10/12/2022**