Perancangan Sistem Pengelolaan Dokumen Dengan Menerapkan Symmetric Key Encryption Berbasis Web

Putu Adi Surya Kusuma[1)], Putu Desiana Wulaning Ayu[2)], I Putu Gede Abdi Sudiatmika[3)]
Program Studi Sistem Komputer
Institut Teknologi dan Bisnis STIKOM Bali
Denpasar, Indonesia
e-mail: putuadisuryakusuma@gmail.com[1], wulaning_ayu@stikom-bali.ac.id[2],
sudiatmika.abdi@gmail.com[3]

Abstrak

Berkembangnya teknologi yang cepat pada era digital membawa manfaat ke dalam beberapa bidang pekerjaan manusia, salah satunya adalah dalam bidang pengelolaan dokumen. Teknologi mampu mengubah bentuk dokumen yang pada awalnya bersifat tradisional dan kaku, menggunakan kertas dan tinta sebagai sarananya, menjadi dokumen dalam bentuk digital yang dapat dikelola dengan bantuan perangkat elektronik seperti komputer yang di dalamnya sudah terpasang sistem yang mampu mengelola dokumen sesuai keinginan pengguna. Bentuk dokumen digital memberikan manfaat berupa fleksibilitas yang tinggi ketika proses pengelolaan terjadi. Terlepas dari manfaat yang ditawarkan, terdapat ancaman yang dapat memberikan dampak buruk bagi dokumen digital. Beberapa ancaman tersebut datang dari aspek keamanan, kerahasiaan, dan juga keaslian isi dari dokumen tersebut. Dalam satu dekade terakhir, sering terdengar kasus penyalahgunaan dokumen resmi untuk kepentingan pribadi yang umumnya melanggar hukum. Kasus lain yang juga umum ditemukan adalah seperti pencurian dan juga sabotase pada isi dokumen. Dengan bantuan teknologi, kemungkinan terjadinya ancaman-ancaman yang disebutkan sebelumnya dapat ditekan. Salah satu cara mencegah terjadinya tindakan kejahatan pada dokumen adalah dengan mengimplementasi proses enkripsi sebagai lapisan keamanan tambahan pada sistem yang dikhususkan untuk melakukan kegiatan pengelolaan dokumen. Penelitian ini diharapkan dapat menghasilkan sebuah rancangan berupa gambaran dan rencana sistem yang akan dibuat dengan berbasis web dengan menggunakan prinsip enkripsi simetris pada tiap dokumen yang dikelola.

Kata kunci: *Dokumen, Teknologi, Digital, Sistem, Web, Enkripsi*

1. Pendahuluan

Dokumen merupakan sebuah hal yang sudah awam ditemukan di masa yang menunjukan keadaan dimana berbagai macam informasi tersebar secara mudah, luas dan cepat. Istilah dokumen dan informasi tidak terpisahkan, karena dokumen sendiri merupakan representasi dari sejumlah informasi yang dikumpulkan berdasarkan fakta dan bukti yang akan digunakan sebagai dasar untuk mendukung kebenaran suatu hal, yang kemudian dituangkan ke dalam sebuah media [1].

Perkembangan teknologi yang pesat tidak hanya mempengaruhi kecepatan dan kemudahan akses terhadap informasi, tetapi juga memperkenalkan media-media baru yang memanfaatkan teknologi dan alat elektronik dalam pengaplikasiannya. Saat ini, dokumen yang memanfaatkan alat elektronik sudah umum dijumpai, seperti contoh dokumen yang diformat ke dalam bentuk dokumen elektronik atau digital dengan bantuan sistem aplikasi yang bekerja pada komputer.

Lahirnya dokumen elektronik meningkatkan fleksibilitas dokumen untuk digunakan dalam berbagai macam keperluan dan tujuan dalam sejumlah bidang pekerjaan. Informasi yang tertuang di dalamnya menentukan jenis dan tujuan dari dokumen tersebut. Selain fakta dan bukti, sebuah dokumen biasanya juga berkaitan dengan data, perintah, karya, pengetahuan, serta dokumen lainnya. Tidak jarang juga bahwa dokumen yang dibuat akan ditujukan kepada pihak atau orang lain. Situasi ini menandakan bahwa sebuah dokumen mengandung informasi yang penting dan harus terjaga keaslian dan kerahasiannya. Dokumen akan lebih dipercaya jika informasi yang tertuang di dalamnya memiliki tingkat integritas dan privasi yang tinggi, sehingga pihak yang terkait, terutama pihak yang dituju atau yang akan menerima dokumen tersebut tidak akan meragukan keasliannya. Ketika privasi dan integritas menjadi sebuah prioritas yang ingin dijaga, maka dibutuhkan tindakan yang diharapkan dapat memberikan keamanan lebih terhadap dokumen elektronik tersebut.

Pada kenyataannya, harapan tersebut masih belum dapat sepenuhnya terpenuhi. Tindakan keamanan yang diberikan terhadap dokumen elektronik masih terbilang minim, bahkan seringkali sebuah dokumen elektronik tidak diberikan tindakan keamanan dalam bentuk apapun. Seperti yang sering dijumpai pada instansi dan kantor-kantor kecil, dimana pertukaran dokumen digital antar departemen di dalam instansi tersebut sering terjadi. Umumnya pertukaran dokumen elektronik dilakukan dengan menggunakan media penyimpanan eksternal seperti *flash drive* yang digunakan secara massal secara bergantian. Hal ini menimbulkan celah keamanan pada saat proses pertukaran dokumen digital berlangsung. Celah yang dimaksud adalah meningkatnya resiko kehilangan sebuah dokumen yang dapat disebabkan oleh beberapa faktor, seperti *human error* dan virus komputer, serta meningkatnya resiko terjadinya sabotase, spionase dan pencurian informasi yang dilakukan oleh pihak ketiga.

Terdapat sebuah penelitian yang dapat mendukung masalah ini. Pada tahun 2020, Simon Baechler melakukan penelitian dengan judul "Document Fraud: Will Your Identity Be Secure In The Twenty-First Century?". Pada penelitiannya, Simon mengutarakan penggunaan dokumen palsu dalam aktivitas kriminal sudah semakin luas, mulai dari penipuan dokumen keuangan hingga terorisme. Perkembangan teknologi memaksa penjahat untuk bertindak lebih kreatif dalam menjalankan aksi jahatnya [2].

Untuk mencegah tindakan kejahatan tersebut, maka perlu dibuatkan sebuah sistem yang tidak hanya menawarkan kemudahan dan kecepatan dalam proses pengelolaan (pertukaran/penyimpanan) dokumen, tetapi juga menghadirkan keamanan yang tinggi. Dan dalam kasus ini, sistem pengelolaan dokumen berbasis web dengan menerapkan *symmetric key encryption* dianggap mampu untuk menyelesaikan permasalahan yang disebutkan sebelumnya. Sistem berbasis web menawarkan fleksibilitas terhadap perangkat yang dapat menggunakan sistem tersebut. Karena pada dasarnya, sistem berbasis web dapat diakses dari berbagai macam perangkat selama perangkat tersebut memiliki aplikasi *browser*. Sistem berbasis web dirasa tepat untuk diimplementasi sesuai dengan situasi ruang lingkup kerja di kantor maupun instansi kecil, dimana jenis perangkat yang digunakan bervariasi.

2. Metode Penelitian

2.1 Metode Pengumpulan Data

2.1.1 Observasi

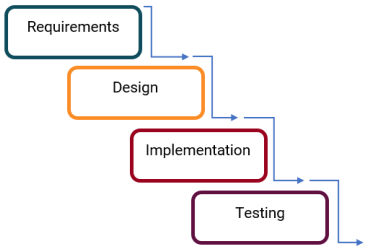
Dalam penelitian ini, penulis melakukan observasi pada salah satu instansi kecil pemerintahan yaitu Kantor Kelurahan Jimbaran pada saat penulis melaksanakan program kerja praktek di tempat tesebut. Observasi yang dilakukan penulis adalah dengan mengamati langsung kegiatan sehari-hari yang berkaitan dengan tugas kepemerintahan, baik itu alur kerja maupun hal-hal yang dikerjakan.

2.1.2 Wawancara

Pada penelitian ini, penulis melakukan proses wawancara terhadap salah satu narasumber di Kantor Kelurahan Jimbaran, beliau adalah Ibu Ni G.A.A. Mirah Dwipayanti, SE. Beliau menjabat sebagai Sekretaris Kelurahan yang bekerja di bawah pengawasan langsung dari Lurah. Beliau juga merupakan Pembina penulis pada pelaksanaan program kerja praktek. Proses tanya jawab yang dilakukan penulis dengan narasumber tidak dilakukan dalam sehari, tetapi dilakukan selama periode kerja praktek berlangsung. Kemudian penulis mengumpulkan pertanyaan yang pernah penulis ajukan beserta dengan tanggapan atau jawaban yang pernah diberikan oleh narasumber lalu menggabungkan keduanya, sehingga mendapatkan data dan informasi yang dapat mendukung proses penelitian ini.

2.2 Metode Perancangan Sistem

Dalam perancangan sistem pada artikel penelitian ini, penulis memutuskan untuk menggunakan metode *waterfall* sebagai metode perancangan sistem. Metode *waterfall* atau sering disebut sebagai *waterfall* model, merupakan sebuah metode perancangan sistem yang berurutan yang memiliki alur seperti layaknya sebuah air terjun. Alur dari perancangan sistem bergerak dari fase paling awal hingga fase terakhir secara berurutan. Sebelum bergerak atau pindah ke fase selanjutnya, perancang sistem harus sudah menyelesaikan hal-hal yang berkaitan dengan fase yang sedang dikerjakannya, jika dirasa sudah lengkap, selanjutnya perancang sistem dapat lanjut ke fase selanjutnya. Sejauh ini terdapat empat fase umum yang dimiliki oleh metode waterfall ini [3], yaitu sebagai berikut:



Gambar 1. Metode Perancangan Sistem Waterfall

Artikel penelitian ini berfokus terhadap tahap perancangan atau perencanaan, yang dimana pada *Waterfall* Model akan berfokus terhadap dua fase pertama yaitu *Requirements* dan *Design.*

3. Hasil dan Pembahasan

3.1 Analisa Kebutuhan Sistem

3.1.1 Kebutuhan Fungsional

a. Sistem dapat digunakan untuk melakukan proses *sign-up*
b. Sistem akan melakukan proses validasi dalam aktivitas *log-in* yang dilakukan oleh pengguna.
c. Sistem dapat digunakan untuk mengelola dokumen digital yang meliputi proses *send*, *download*, dan *delete*.
d. Sistem akan melakukan proses enkripsi dengan menerapkan sebuah algoritma terhadap nama file dari dokumen yang dikirim, sehingga nama file yang ditampilkan pada sistem dan yang disimpan akan berbentuk *cipher-text*
e. Sistem akan memberikan *key* secara acak ke setiap dokumen digital yang terdapat di dalam sistem. *Key* ini akan digunakan saat algoritma enkripsi berjalan.

3.1.2 Kebutuhan Non-Fungsional

a. Tersedianya perangkat komputer yang akan berperan sebagai server, tempat sistem tersebut nantinya beroperasi. Perangkat server yang dibutuhkan diharapkan dalam keadaan aktif selama 24 jam, atau setidaknya berjalan selama jam kerja berlangsung.
b. Perangkat server diharapkan memiliki spesifikasi yang memadai. Spesifikasi yang diharapkan adalah seperti menggunakan processor Intel Xeon, memiliki RAM setidaknya 16GB, dan menggunakan SSD sebagai perangkat penyimpanan yang memiliki kapasitas setidaknya 1TB.
c. Tersedianya perangkat komputer yang akan mengakses sistem tersebut (*client/user)*
d. Perangkat komputer *user* diharapkan berjalan pada sistem operasi Windows dengan versi Windows yang diharapkan adalah Windows 7 hingga versi di atasnya
e. Perangkat komputer *user* juga diharapkan memiliki browser yang sudah terinstall di dalamnya, browser yang disarankan adalah Google Chrome
f. Tersedianya sistem jaringan komputer lokal yang dapat menghubungkan komputer server dengan komputer pengguna.

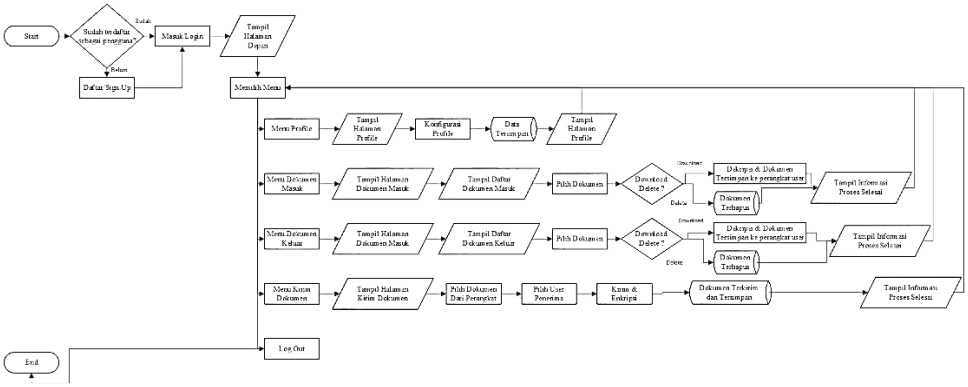
3.2 Ilustrasi Alur dan Penjelasan Sistem

Sistem berjalan diawali dengan tahap *log-in*, pada tahap ini proses verifikasi *user* terdaftar terjadi. Pengguna akan diminta untuk memasukan kredensial *user* berupa *username* dan *password*. Jika kedua kredensial yang dimasukan oleh pengguna salah, maka pengguna diminta untuk melakukan proses pendaftaran atau *sign-up*. Jika kedua kredensial tersebut bersifat valid, artinya pengguna tersebut merupakan *user* terdaftar dan akan diarahkan ke halaman utama dari web. Terdapat lima menu pada sistem ini, yaitu menu "Profile", "Kirim Dokumen", "Dokumen Masuk", "Dokumen Keluar", dan "Log-Out". Halaman "Profile" akan ditetapkan sebagai halaman utama dari web secara *default-by-system.* Pada menu "Profile", *user* dapat melakukan kegiatan konfigurasi pada informasi yang berkaitan dengan identitas *user*. Setelah melakukan konfigurasi, informasi terbaru akan disimpan ke dalam *database* dan sistem akan menampilkan halaman "Profile" dengan informasi yang telah diperbaharui.

Pada menu "Kirim Dokumen", *user* dapat mengirim sebuah dokumen ke *user* yang akan dituju. Proses pengiriman diawali dengan tahap pemilihan dokumen yang akan dikirim, kemudian dilanjutkan dengan tahap pemilihan user penerima (*receiver*). *User* diperbolehkan untuk mengirim lebih dari satu dokumen secara bersamaan, hal serupa juga berlaku untuk penentuan *user* penerima, dimana *user* dapat mengirim dokumen ke beberapa *user* penerima secara bersamaan, hal ini akan membantu *user* ketika ingin

mengirimkan dokumen yang dikategorikan sebagai *broadcast-document*. Pada saat *user* mengirim dokumen, sistem akan secara langsung melakukan proses enkripsi terhadap judul dokumen yang dikirim. Sistem akan menentukan sebuah *key* yang akan digunakan pada perhitungan algoritma dari proses enkripsi yang berjalan. Kemudian dokumen yang telah melalui proses enkripsi akan diteruskan ke user penerima dan disimpan ke dalam *database* sistem. Dokumen yang tersimpan akan ditampilkan ke dalam bentuk *ciphertext*.

Selanjutnya terdapat dua menu yang memiliki tujuan yang ekuivalen, yaitu menampilkan daftar dari dokumen-dokumen yang tersimpan pada database sistem ke dalam bentuk tabel. Kedua menu tersebut adalah menu "Dokumen Masuk" dan "Dokumen Keluar". Sedikit perbedaan dari kedua menu ini adalah jenis dokumen yang ditampilkan. Pada halaman "Dokumen Masuk", sistem akan menampilkan semua dokumen yang diterima oleh *user* dari *user* lain yang berperan sebagai pengirim. Sedangkan pada halaman "Dokumen Keluar", hal sebaliknya terjadi, sistem menampilkan semua dokumen yang telah dikirim oleh *user* kepada *user* penerima. Pada kedua halaman ini, *user* dapat melakukan dua kegiatan pengelolaan dokumen, yaitu *download* dan *delete*. Kedua kegiatan ini diterapkan ke dalam bentuk *button* yang disediakan di akhir baris dokumen pada tabel. Ketika user melakukan salah satu dari kedua kegiatan pengelolaan tersebut, sistem akan melakukan proses dekripsi kepada dokumen yang akan dikelola, mengingat seluruh dokumen yang tersimpan ditampilkan ke dalam bentuk *ciphertext*. Proses *download* memungkinkan user untuk mengunduh dokumen yang tersimpan di dalam *database* sistem dan dipindahkan ke sistem penyimpanan perangkat yang digunakan user. Sedangkan proses *delete* akan dilakukan user ketika sebuah dokumen ingin dihapus dari *database* sistem. Jika user ingin keluar dari sistem dan kembali ke halaman *login*, *user* dapat memilih menu "*Log Out*". Sistem juga akan mengeluarkan *user* dari sistem ketika user dalam kondisi *idle* atau tidak ada aktivitas pada sistem selama lima menit. Berikut merupakan ilustrasi alur sistem yang ditampilkan dalam bentuk *flowchart*:

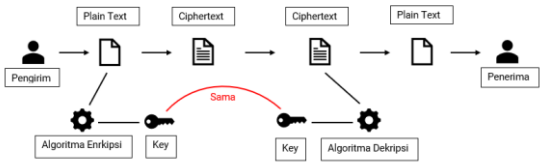


Gambar 2. *Flowchart* Sistem

3.3 Rencana Implementasi Enkripsi

3.3.1 Symmetric Key Encryption

Symmetric Key Encryption adalah salah satu jenis enkripsi yang menggunakan *key* yang sama pada saat proses enkripsi dan dekripsi berlangsung. *Key* tersebut diperoleh dari sistem secara acak. *Key* ini selanjutnya digunakan untuk menjalankan algoritma yang digunakan dalam proses enkripsi dan juga dekripsi [4]. Proses enkripsi akan dilakukan pada dokumen yang akan dikirim oleh *user*, sedangkan proses dekripsi akan dilakukan ketika *user* akan melakukan proses *download* maupun *delete*.

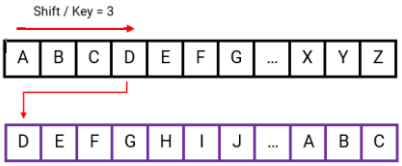


Gambar 3. Ilustrasi Proses *Symmetric Key Encryption*

3.3.2 Algoritma *Caesar Cipher*

Algoritma *Caesar Cipher* bekerja dengan menggunakan konsep subsitusi atau pertukaran. Setiap huruf pada pesan yang masih dalam bentuk *plaintext* akan disubstitusi dengan kumpulan huruf yang telah

melalui proses shift atau pergeseran sebelumnya. Algoritma *Caesar Cipher* menggunakan sebuah *key*, dimana pergeseran terhadap urutan alfabet ditentukan berdasarkan *key* yang digunakan [5].



Gambar 4. Ilustrasi Algoritma Caesar Cipher

Dalam penerapannya, algoritma *Caesar Cipher* akan diimplementasikan ke dalam konsep matematika, dimana setiap huruf akan direpresentasikan ke dalam bentuk *array* dan setiap huruf memiliki nomor indeksnya masing-masing yang dimulai dari bilangan nol. Nomor indeks ini yang nantinya akan digunakan dalam perhitungan dengan menggunakan sebuah rumus matematika sederhana yang juga akan melibatkan *key* yang sudah ditentukan sebelumnya. Adapun indeks dan juga rumus yang digunakan dalam algoritma Caesar Cipher adalah sebagai berikut:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Enkripsi = (Indeks Huruf + Key) modulus 26
Dekripsi = (Indeks Huruf – Key) modulus 26

Gambar 5. Indeks dan Rumus Algoritma Caesar Cipher

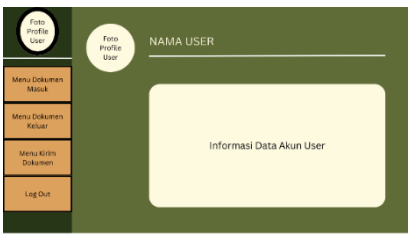
Rumus di atas dapat dicontohkan dengan menggunakan nilai 3 sebagai *key*, dan huruf C akan melalui proses enkripsi. Indeks dari huruf C adalah 2, jadi Indeks dijumlahkan dengan *key* menghasilkan nilai 5, kemudian 5 modulus 26 menghasilkan nilai 5. Maka huruf C setelah melalui proses enkripsi akan berubah menjadi huruf pada indeks 5, yaitu huruf F. Hasil penjumlahan yang melalui proses modulus bertujuan untuk menjaga agar hasil perhitungan tetap di rentang indeks 0 hingga 25. Sebagai contoh jika huruf X akan melalui proses enkripsi, nilai *key* masih sama yaitu 3. Indeks huruf X adalah 23, hasil penjumlahan indeks huruf X dengan *key* adalah 26, sedangkan tidak ada huruf yang memiliki indeks dengan nilai 26. Maka dari itu diperlukan modulus, nilai 26 modulus 26 menghasilkan nilai 0, jadi huruf X setelah proses enkripsi akan berubah menjadi huruf pada indeks 0, yaitu huruf A.

3.4 Rencana Implementasi Web

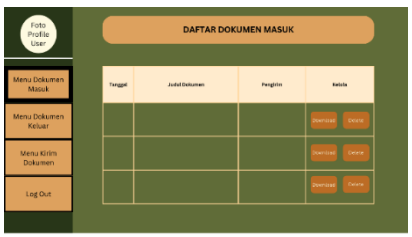
3.4.1 Struktur Jaringan dan Teknologi

Web akan direncanakan berjalan dalam struktur jaringan lokal (*localhost*), dimana web akan dijalankan pada *server* yang nantinya akan diakses melalalui perangkat pengguna (*client*). Web akan dibangun dengan menggunakan beberapa teknologi. HTML, CSS, dan JavaScript akan digunakan untuk membangun bagian *front-end* dari web, sedangkan untuk *back-end* akan dibangun dengan teknologi Node.js. Bagian *database* akan menggunakan teknologi mongoDB yang bertugas sebagai tempat penyimpanan data *user* serta file dokumen.

3.4.2 Design Tampilan Web (Prototype)

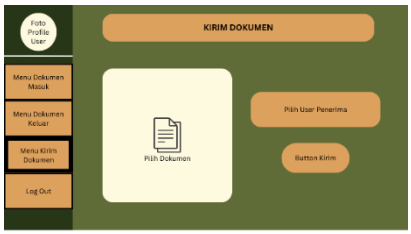


Gambar 7. Design Menu Profile



Gambar 8. Design Menu Dokumen Masuk

Gambar 9. Design Menu Dokumen Keluar



Gambar 10. Design Menu Kirim Dokumen

4. Kesimpulan

Pada penelitian ini hanya membahas perancangan atau perencanaan dari sebuah sistem yang dibuat untuk menangani ancaman keamanan yang dapat terjadi dalam proses pengelolaan dokumen. Penelitian ini dapat dibawa ke langkah lebih lanjut sesuai dengan metode perancangan *waterfall.* Dari hasil dan juga pembahasan yang sudah dijabarkan di atas, dapat ditarik beberapa kesimpulan sebagai berikut :

- Rancangan "Sistem Pengelolaan Dokumen Dengan Menerapkan Symmetric Key Encryption Berbasis Web" dapat diselesaikan dengan menggunakan metode perancangan *waterfall* yang berfokus pada dua lapisan teratas dari *waterfall model.*
- Implementasi enkripsi dengan menerapkan *Symmetric Key Encryption* dirasa mampu menangani masalah dan ancaman keamanan pada proses pengelolaan dokumen.
- Sistem berbasis web dirasa sesuai jika diimplementasi pada kantor atau instansi kecil, mengingat kondisi lingkungan kerja yang melibatkan lebih dari satu jenis perangkat elektronik.
- Sistem akan dijalankan pada struktur jaringan lokal (*localhost).* Hal ini dapat mempersempit jangkauan sistem, sehingga hanya dapat diakses oleh perangkat yang sudah terverifikasi untuk masuk ke dalam jaringan lokal tersebut.

Daftar Pustaka

[1] Merriam-Webster. (n.d.). Document. In Merriam-Webster.com dictionary. Retrieved October 2, 2023, from https://www.merriam-webster.com/dictionary/document

[2] Baechler, S. (2020). Document fraud: Will your identity be secure in the twenty-first century?. European Journal on Criminal Policy and Research, 26(3), 379-398.

[3] Ernest Kwame, A., Mensah Martey, E., & Gilbert Chris, A. (2017). Qualitative Assessment of Compiled, Interpreted and Hybrid Programming Languages. Communications on Applied Electronics, 7(7).

[4] Surya, E., & Diviya, C. (n.d.). A Survey on Symmetric Key Encryption Algorithms. International Journal of Computer Science & Communication Networks, 2(4).

[5] Cracking the Code — Central Intelligence Agency (CIA). (n.d.). CIA's Open Government. Retrieved January 16, 2023, from https://web.archive.org/web/20201226065538/https://www.cia.gov/news-information/featured-story-archive/2007-featured-story-archive/cracking-the-code.html