Penerapan Kombinatorial dalam Multifactor Authentication

Vanessa Rebecca Wiyono - 13521151
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13521151@std.stei.itb.ac.id

***Abstract*—Teori kombinatorial merupakan salah satu bahasan dari bidang matematika diskrit yang sangat populer karena aplikasinya merekat erat dengan berbagai hal dalam dunia nyata, terlebih pada ilmu komputer, teori informasi, serta statistika. Penggunaan kombinatorial juga tak lepas dari autentikasi dan kerahasiaan, dengan contoh paling sederhana adalah enkripsi terhadap data-data penting dalam ukuran panjang yang bervariasi. Tujuan dari enkripsi tersebut adalah untuk meningkatkan kerahasiaan atas data penting pengguna seperti kata sandi, identitas pribadi, serta hal yang memang bersifat rahasia. Masih terkait dengan keamanan dan autentikasi, teori kombinatorial juga digunakan dalam autentikasi biometrik yang biasanya menyimpan data terkait sidik jari maupun iris mata seseorang karena setiap orang memiliki sidik jari dan iris mata yang berbeda. Baik kata sandi, enkripsi, maupun biometrik kemudian diimplementasikan dalam *Multifactor Authentication (MFA)* yang merupakan sistem keamanan dengan perlindungan lebih tinggi karena mengharuskan penggunanya untuk melakukan beberapa tahap autentikasi secara bertahap.**

Keywords*—Kombinatorial, Enkripsi, Biometrik, *Multifactor Authentication

I. PENDAHULUAN

Saat ini isu terkait modus penipuan dengan alibi kurir mengirimkan pesan berupa file pdf maupun foto yang ternyata merupakan aplikasi pembobol data *mobile banking* sedang hangat-hangatnya menjadi perbincangan di Indonesia. Penipu akan berpura-pura menjadi kurir yang mengantar paket dan kemudian memberi lampiran dengan nama file 'LIHAT foto Paket' yang formatnya terlihat seperti gambar jpg maupun jpeg, namun ketika dibuka ternyata bukan merupakan gambar dan justru merupakan aplikasi yang dapat meretas data korban. Aplikasi tersebut akan langsung terunduh secara otomatis saat korban meng-*click* lampiran tadi.

Peristiwa tak menyenangkan ini tentu hanya merupakan salah satu dari sekian banyak peristiwa serupa yang sudah sering terjadi sebelumnya, namun tentu dilakukan dengan modus pendekatan yang berbeda-beda. Walaupun modusnya sangat beragam, perlu diketahui bahwa dasar dari penipuan ini tak jauh dari aktivitas peretasan dengan metode *Keylogger* dan *Man in the Middle Attack*.

Keylogger merupakan peretasan yang dilakukan dengan cara merekam aktivitas serta data pengguna tanpa sepengetahuan pengguna (tak terdeteksi). Peretas dapat mengetahui segala aktivitas korban mulai dari merekam segala tombol yang diketikkan korban, melihat isi chat korban, mengetahui riwayat pencarian korban, serta melakukan *screen capture*. Dengan demikian peretas memiliki akses pada segala data sensitif korban, termasuk kata sandi dan data *banking* pribadi.

Berbeda dengan *Keylogger* yang merekam segala aktivitas korban, *Man in the Middle Attack* merupakan keadaan dimana peretas memposisikan dirinya diantara korban dengan pihak lain yang sedang berkomunikasi dengan korban. Dalam kasus ini, peretas dapat mencegat serta mengubah perjalanan data korban. Contohnya adalah ketika korban menggunakan aplikasi perbankan, melakukan transaksi secara daring pada aplikasi maupun situs tertentu, melakukan login, dan lain-lain. Tidak hanya mencuri data penting korban, serangan dengan jenis *Man in the Middle* ini juga dapat memasukkan serangan *Malware*. [8], [9]

Untuk mengatasi peretasan dengan berbagai macam modus, maka diperlukan sistem keamanan tinggi yang lebih menjamin keamanan data pengguna. Salah satu hal yang dapat diterapkan guna meningkatkan keamanan adalah dengan menerapkan *Multifactor Authentication*, yang antara lain adalah proses autentikasi yang dilakukan dengan beberapa langkah. Tidak hanya memasukkan kata sandi, pengguna juga diharuskan untuk melakukan berbagai autentikasi lain seperti kode verifikasi yang biasa dikirim ke nomor ponsel atau *e-mail*, memasukkan PIN, memasukkan biometric seperti sidik jari atau pengenalan wajah, dan masih banyak lagi.

Penerapan *Multifactor Authentication* sangat erat dengan teori kombinatorial karena baik kata sandi, PIN, hingga tentikasi biometrik seluruhnya merupakan implementasi dari teori kombinatorial. Semakin banyak kemungkinan dalam membentuk kata sandi, maka semakin baik kata sandi tersebut karena mempersulit orang lain untuk membobolnya. Dalam hal ini, terlihat jelas peran teori kombinatorial yang digunakan untuk menghitung kekuatan kata sandi dari serangan *brute force*. Selain itu, penggunaan autentikasi biometrk juga merupakan implementasi nyata dari kombinatorial, dimana semua orang memiliki atribut biometrik yang unik sehingga keamanan biometric dianggap kuat karena menghasilkan kombinasi dengan jumlah yang sangat banyak dan terus bertambah.

II. TEORI DASAR

1. Teori Kombinatorial

Kombinatorial merupakan salah satu bahasan dari cabang iilmu Matematika Diskrit yang mempelajari pengaturan terhadap objek-objek dan menghasilkan solusi berupa banyak cara pengaturan objek-objek tersebut tanpa melakukan enumerasi terhadap setiap kemungkinan. Pada teori kombinatorial, erdapat dua macam kaidah dasar yang digunakan untuk menghitung seluruh cara pengaturan objek. Kedua kaidah tersebut antara lain adalah kaidah perkalian dan kaidah penjumlahan. [1], [2], [7]

A. Kaidah Perkalian (*rule of product*)

Kidah perkalian digunakan saat ada dua kejadian atau lebih yang terjadi secara bersamaan. Misal terdapat kejadian P dan Q yang dilakukan secara bersamaan, maka jumlah kejadian yang mungkin terjadi dapat diperoleh melalui perhitungan P x Q. P disini menunjukkan jumlah kemungkinan terjadinya kejadian P dan Q menunjukkan jumlah kemungkiann terjadinya kejadian Q. Jika ada n buah percobaan, maka banyak hasil percobaan yang mungkin terjadi adalah :

$$p1 \times p2 \times p3 \times \ldots \times pn$$

B. Kaidah Penjumlahan (*rule of sum*)

Kaidah penjumlahan digunakan untuk menghitung banyak cara perhitungan dua kejadian atau lebih yang tidak terjadi secara bersamaan. Misal terdapat P cara untuk terjadinya kejadian p dan Q cara untuk terjadinya kejadian Q, maka akan terdapat P + Q cara pengurutan jika percobaan Q atau P dilakukan. Jika ada n buah percobaan, maka banyak hasil percobaan yang mungkin terjadi adalah :

$$p1 + p2 + p3 + \ldots + pn$$

Selain kedua kaidah tersebut, terdapat pula dua acara untuk menghitung kombinatorial. Kedua cara perhitungan tersebut antara lain adalah permutasi dan kombinasi.

Permutasi

Permutasi merupakan salah satu bentuk umum dari kombitorial yang membahas cara penyusunan sekelompok objek dimana urutan objek diperhatikan dan dianggap penting. Dengan kata lain, urutan keberadaan suatu objek diperhitungkan dalam permutasi. Salah satu contoh kasus yang penyelesaiannya menggunakan permutasi adalah sistem *ranking* dikelas, dimana urutan harus diperhitungkan karena peringkat pertama berbeda dengan peringkat kedua. Berbeda dengan kasus pengaturan piket kelas, dimana urutan siswa tidak penting karena solusi tetap dianggap sama apabila mendapat sesi / waktu piket yang sama.

Permutasi dapat dihitung menggunakan rumus:

$$P_r^n = \frac{n!}{(n-r)!}$$

Kombinasi

Lain halnya dengan permutasi yang memperhatikan urutan objek, urutan objek pada kombinasi dianggap tidak penting sehingga tidak diperhitungkan. Dengan kata lain, kombinasi merepresentasikan permutasi yang tidak memperhatikan urutan. Seperti kasus yang telah disinggung diatas, pengaturan piket kelas merupakan contoh dari kombinasi karena urutan tidak diperhatikan (urutan disini menunjukkan urutan orang terpilih. Misal, orang yang dipilih pertama adalah A kemudian B dan diikuti dengan C, namun ketiganya mendapat jam piket yang sama). Selain pengaturan piket, contoh lain dari kombinasi adalah dalam menghitung kejadian untuk masuk kedalam suatu organisasi.

Kombinasi dapat dihitung menggunakan rumus:

$$C_r^n = \frac{n!}{r!\,(n-r)!}$$

Permutasi dan Kombinasi Bentuk Umum

Permutasi dan kombinasi bentuk umum merupakan perhitungan yang dilakukan ketika kemungkinan seluruh penyusunan objek ingin dihitung bersama dengan beberapa objek yang sama. Contoh paling sederhananya adalah menghitung kemungkinan terambilnya bola, namun terdapat beberapa bola yang berwarna sama. Dalam kasus ini, perhitungan dilakukan dengan membagi banyak cara penyusunan total dengan banyak cara penyusunan masing-masing objek yang memiliki atribut sama.

Permutasi dalam bentuk umum dapat dihitung dengan menggunakan rumus:

$$P(n, n_1, n_2, \ldots, n_k) = \frac{n!}{n_1!\, n_2! \ldots n_k!}$$

Kombinasi dalam bentuk umum dapat dihitung dengan menggunakan rumus:

$$C_{n_1}^{n} C_{n_2}^{n-n_1} C_{n_3}^{n-n_1-n_2} \ldots C_{n_k}^{n_k}$$

Walaupun rumus untuk keduanya terlihat berbeda,

namun hasil yang didapat akan sama.

2. Peluang

Peluang diskrit atau yang juga dikenal sebagai probabilitas merupakan kemungkinan terjadinya suatu kejadian dengan jumlah anggota yang terbatas pada suatu ruang sampel. Nilai perluang diskrit berada pada skala 0 sampai 1, dimana 1 menunjukkan peluang yang sangat besar atau bisa dikatakan pasti terjadi. Perhitungan peluang diskrit menggunakan kaidah permutasi dan kombinasi, dimana hasil dari kaidah tersebut kemudian dibagi dengan jumlah seluruh kemungkinan yang mungkin terjadi. Salah satu contoh konkrit dari peluang adalah aktivitas pelemparan dadu dimana sang pelempar bisa menghitung berapa kemungkinan agar dadunya menghasilkan angka yang genap, Peluang kemudian dihitung dengan cara menghitung jumlah kemungkinan dadu bernilai genap {2, 4, 6} dan membaginya dengan seluruh kemungkinan yang ada {1, 2, 3, 4, 5, 6}. Perhitungan tersebut menunjukkan bahwa peluang yang dimiliki adalah sebesar 0.5 atau 50% (dalam persentase)

Peluang dapat dihitung menggunakan rumus:

$$p(E) = \frac{|E|}{|S|} = \sum_{x_i \in E}^{n} p(x_i)$$

P(E) = peluang kejadian E
E = kejadian E
S = ruang sampel S

3. *Multifactor Authentication*

Autentikasi multi-faktor (MFA) merupakan mekanisme keamanan multilangkah yang mewajibkan penggunanya untuk melakukan lebih dari satu autentikasi untuk masuk / *login* kedalam suatu akun atau untuk melakukan suatu transaksi ketimbang hanya sekedar memasukkan kata sandi. MFA melakukan penggabungan terhadap dua atau lebih kredensial independen seperti kata sandi, token, kode numerik, serta biometrik dengan tujuan untuk menciptakan pertahanan berlapis sehingga akan lebih sulit bagi seseorang untuk melakukan peretasan. Ibaratnya jika salah satu faktor autentikasi telah berhasil dihancurkan, maka peretas tidak langsung sampai pada data sensitif pengguna, melainkan harus melewati lapisan autentikasi lainnya terlebih dahulu. Terkait dengan fungsinya, MFA mengambil peran penting dalam platform identitas pelanggan dan manajemen akses atau yang dikenal juga dengan istilah *Customer Identity Access Management (CIAM)*. [3], [6], [10]

Sebagai contoh, salah satu penggunaan autentikasi multi faktor dalam kehidupan nyata adalah ketika seseorang melakukan transaksi di mesin ATM, dimana pengguna diharuskan untuk menggesekkan kartu yang bersifat unik (setiap kartu memiliki nomornya masing-masing) dan kemudian harus memasukkan PIN. Hal ini merupakan penggabungan antara kredensial berupa PIN dengan perangkat keras, yaitu kartu ATM karena memiliki wujud fisik. Contoh lain yang tidak menerapkan penggunaan perangkat keras adalah proses autentikasi pembayaran ketika melakukan transaksi secara daring pada aplikasi tertentu. Selain memasukkan PIN, biasanya proses pembayaran juga disertai dengan tahap verifikasi yaitu dengan memasukkan kode numerik unik yang dikirimkan pada ponsel / *e-mail* pemilik akun. Terlihat jelas bahwa masing-masing dari kedua contoh tersebut melakukan penggabungan antara dua kredensial dari kategori yang berbeda guna meningkatkan keamanan. Apabila proses autentikasi dilakukan dengan memasukkan dua kata sandi yang berbeda, maka proses tersebut tidak tergolong sebagai autentikasi multi-faktor karena keduanya merupakan kredensial dengan kategori yang sama, yaitu kata sandi.

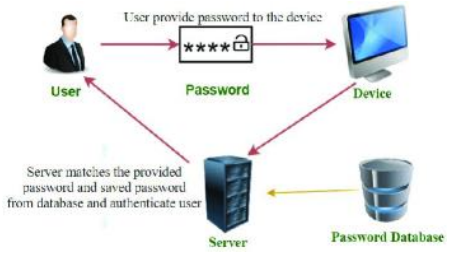
Pasalnya, terdapat 3 jenis faktor utama dalam melakukan MFA, yang antara lain adalah:

- Hal yang bersifat sebagaai pengetahuan, contoh: kata sandi atau PIN
- Hal yang bersifat kepemilikan, contoh: kartu, ponsel
- Hal yang bersifat biometric, contoh: Sidik jari, pengenalan wajah, iris mata

4. Kata Sandi dan PIN

Kata Sandi atau yang biasa dikenal sebagai *password* merupakan kombinasi alfanumerik yang kemudian digunakan dalam melakukan proses autentikasi. Kata sandi bersifat rahasia, sehingga akan dilakukan enkripsi ketika pengguna memasukkan kata sandi. Karena merupakan kombinasi alfanumerik, panjang dan variasi karakter merupakan kunci penting untuk menggolongkan apakah suatu kata sandi baik atau tidak. Semakin panjang dan semakin variatif karakternya, maka semakin baik pula kata sandi tersebut.

PIN memiliki prinsip dasar yang tak jauh berbeda dari kata sandi, dimana keduanya merupakan kombinasi dan semakin panjang karakternya maka akan semakin baik. Namun yang menjadi pembeda antara PIN dan kata sandi adalah unsur pembentuknya, dimana kata sandi berupa kombinasi alfanumerik sedangkan PIN merupakan kombinasi numerik saja. Berikut contoh gambaran proses validasi PIN.



Gambar 1. User password overview

Sumber: https://www.researchgate.net/figure/Password-authentication-process_fig6_336717897, diakses 8 Desember 2022

5. Biometrik

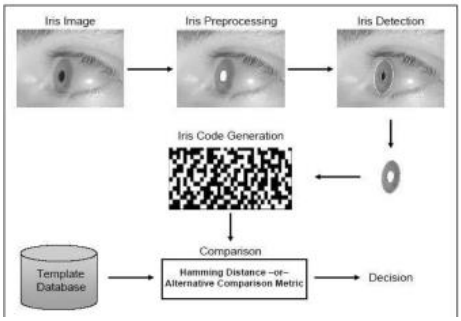
Biometrik merupakan kredensial dengan tingkat keamanan yang lebih tinggi ketimbang jenis kredensial lainnya karena bersifat unik, dimana setiap orang memiliki biometrik yang berbeda dan tidak mungkin bagi seseorang untuk melakukan duplikasi terhadap biometrik orang lain. Salah satu contoh autentikasi biometrik yang penggunaannya paling popular adalah sidik jari. Sidik jari merupakan pola guratan pada kulit manusia yang selalu berbeda pada setiap individu, bahkan anak kembar sekalipun. Maka dari itu, peluang bagi seseorang untuk membobol sistem ini menjadi sangat kecil karena kemungkinan berhasilnya hanya satu dari berjuta-juta orang. Jika dikategorikan menjadi kelas besar, maka terdapat 3 kategori sidik jari manusia, yaitu *arch, loop,* dan *whorl.* [5]

Berikut contoh visualisasinya:

Gambar 2. (kiri ke kanan: arch, whorl, loop)

Sumber: https://attorneyatlawmagazine.com/latestarticles/various-types-fingerprint (diakses 9 Desember 2022)

Contoh kredensial biometrik lainnya, yaitu iris mata:



Gambar 3. Autentikasi biometrik dengan iris mata

Sumber: https://data03.123doks.com/thumbv2/123dok/000/156/156802/20.612.157.493.143.376/gambar-proses-umum-sistem-biometrik-iris-mata.webp (Diakses 9 Desember 2022)

6. Malware

Malicous Software atau biasa dikenal sebagai Malware adalah perangkat lunak yang didesain sedemikian rupa sehingga dapat merusak sistem pertahanan, jaringan, dan server komputer, sehingga dapat "membuka" pintu masuk bagi peretas ke komputer korban. Selain itu, malware juga sering digunakan untuk melakukan pencurian data. Jaringan internet merupakan salah satu jalan masuk utama malware pada sisem komputer, dimana umumnya perangkat lunak ini disisipkan melalui unduhan di situs-situs illegal, iklan (terlebih *pop-up ads*), *email pishing*, dan *broadcast.*

Terdapat berbagai macam jenis Malware yang perlu diwasppadai, antara lain adalah: [14]

- Virus
  Virus merupakan malware yang biasanya muncul melalui unduhan pada sebuah situs, penggunaan USB, dan koneksi jaringan. Seperti Namanya yaitu virus, malware bertipe ini akan bekerja ketika pengguna membuka sebuah dokumen yang telah terinfeksi. Virus dapat melakukan repklikasi dan menyerang sistem komputer pada bagian lain tanpa sepengetahuan pengguna. Tujuan diciptakannya jenis malware ini adalah untuk mengganggu proses kerja sisten serta menghilangkan data, informasi, dan dokumen.

- Adware
  Adware merupakan malware yang biasanya disisipkan pada iklan. Ketika pengguna membuka atau meng-*click* iklan tersebut, maka *spyware* dapat terkirimkan dan merekam seluruh aktivitas pada komputer. Biasanya, malware bertipe ini digunakan untuk mengumpulkan informasi pribadi yang dapat berupa kata sandi, identitas, informasi kartu kredit, dan lain-lain.

- Trojan
  Mirip dengan Adware, Trojan digunakan untuk melihat aktivitas pengguna secara diam-diam. Namun, Trojan tidak disisipkan pada iklan, melainkan melalui penyamaran sebagai sebuah aplikasi yang tidak berbahaya sehingga pengguna akan merasa aman untuk mengunduhnya.

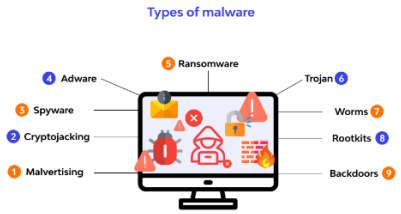
- Worm
  Malware bertipe worm memiliki kemampuan untuk menggandakan diri sehingga sama halnya seperti virus, worm dapat menyebar dengan mudah pada sistem komputer tanpa sepengetahuan pengguna. Maka dari itu, worm tergolong sebagai malware yang cukup berbahaya karena kemampuannya untuk bergerak dan berkembang secara independen.

- Botnet
  Robot Network atau yang bisa disingkat sebagai botnet merupakan sekumpulan bot penyusup jaringan dan sistem komputer yang dapat dikendalikan oleh peretas. Malware bertipe ini dimanfaatkan dalam pengambilan alih control perangkat.

- Ransomware
  Ransomware merupakan salah satu jenis malware

yang paling sering digunakan dalam kejahatan *cyber*, dimana Ransomware dapat mengunci dan menolak pengguna dalam akses sistem komputer serta data di dalamnya. Biasanya, peretas akan meminta uang tebusan pada korban agar sistem komputer mereka dapat terbuka kembali.

Berikut jenis-jenis Malware yang lebih lengkap:



Gambar 4. Jenis-jenis Malware
Sumber: https://www.wallarm.com/what/malware-types-and-detection, diakses 9 Desember 2022

7. Keylogger

Keylogger merupakan *malware* [11] yang merekam aktivitas penekanan tombol pada konsol, kemudian mengirimkan rekaman dari data-data dan aktivitas tersebut pada pihak lain dengan tujuan untuk mengambil data sensitif orang lain secara diam-diam. [12] Umumnya, data yang diambil oleh peretas meliputi kata sandi, *client ID*, isi arsip, serta identitas pribadi yang bersifat rahasia. Saat ini Sebagian besar antivirus masih belum mampu mendeteksi *keylogger*, sehingga akan sulit untuk sadar akan keberadaan *keylogger*.

III. ANALISIS DAN PEMBAHASAN

KOMBINATORIAL DALAM MFA

Autentikasi pada MFA dilakukan secara bertahap pada setiap lapisannya, sehingga bab ini akan membahas penerapan kombinatorial per tahapan MFA.

1. Kombinatorial dalam PIN

PIN menerima masukan berupa kombinasi numerik dengan panjang karakter yang telah ditetapkan. Biasanya, aplikasi *e-commerce* dan perbankan mewajibkan penggunanya untuk memasukkan PIN dengan panjang 6 karakter. Maka dari itu, kita dapat menghitung banyaknya kemungkinan PIN yang dapat terbentuk dengan syarat panjang 6 karakter tersebut. Berikut adalah perhitungannya:

$X_6 = P_1 \times P_2 \times P_3 \times P_4 \times P_5 \times P_6$

Karena karakter numerik yang dapat digunakan berjumlah 10 buah {0, 1, 2, …, 9} sehingga P_i selalu bernilai 10. Dengan asumsi bahwa angka pada setiap digit dibebaskan, maka persamaan dapat diubah menjadi:

$X_6 = 10^6$

Dengan demikian, terlihat jumlah total kemungkinan PIN yang terbentuk sangat banyak, yaitu sebanyak 10^6 dengan banyak percobaan yang biasanya dibatasi hanya 3x. Oleh karena itu, kemungkinan seseorang berhasil menebak PIN orang lain sangat kecil, yaitu sebesar $3 / 10^6$. Karena pembatasan yang ada, maka tidak mungkin bagi seseorang untuk membobol PIN dengan aktivitas *brute force*. Walau peluangnya sangat kecil, namun hal ini masih sering kali menjadi masalah dimana para peretas tetap bisa melakukan peretasan dan mengetahui PIN korban tanpa melakukan *brute force*.

2. Kombinatorial dalam biometrik [4]

Pada bab ini, autentikasi biometrik yang akan dibahas adalah biometrik dengan sidik jari karena penggunaannya yang paling lazim. Terdapat berbagai macam model untuk mengintifikasi dan membandingkan sidik jari manusia antar satu individu dengan yang lainnya, seperti Model Galton (1982), Model Henry (1900), hingga Model Pankanti (2001). Ketiga model tersebut memiliki kesamaan dalam menggolongkan sidik jari berdasarkan detil setiap sidik jari atau yang biasa disebut *minutiae*. Semakin banyak *minutiae*, maka kompleksitasnya semakin tinggi pula sehingga kemungkinan untuk menemukan 2 sidik jari yang sama semakin kecil. Contoh *minutiae* adalah garis yang membelah ke 2 arah (*bifurcation*), serta akhir dari garis (*ridge ending*).

Ekstrasi fitur pada *minutiae* dilakukan dengan pencarian titik-titik *minutiae* dan kemudian dilanjutkan dengan tahap estimasi arah, tahap pendekatan guratan, tahap pembentukan tulang, hingga tahap pendeteksian *minutiae*.

Estimasi arah pada sidik jari dilakukan melalui segmentasi citra menjadi blok-blok yang berukuran lebih kecil dengan ukuran yang sama dan kemudian semua pixel di tiap blok dihitung gradiennya dengan menggunakan rumus:

$$\theta = \frac{1}{2}\tan^{-1}\left(\frac{\sum_{i=1}^{W}\sum_{j=1}^{W} 2G_x(i,j)G_y(i,j)}{\sum_{i=1}^{W}\sum_{j=1}^{W}(G_x^2(i,j) - G_y^2(i,j))}\right)$$

Setelah melakukan estimasi, maka tahap selanjutnya adalah tahap pendekatan guratan yang dilakukan dengan konvulsi citra sidik jari dan melakukan perhitungan nilai *graylevel* dengan rumus:

$$h_t(x,t;u,v) = \begin{cases} -\frac{1}{\sqrt{2\pi\delta}} e^{\frac{u}{\delta^2}}, & if\ u = (v\tan(\theta(x,y)) - \frac{H}{2\cos(\theta(x,y))}), v \in \Omega \\ \frac{1}{\sqrt{2\pi\delta}} e^{\frac{u}{\delta^2}}, if\ u = (v\tan(\theta(x,y))), v \in \Omega \\ 0, otherwise \end{cases}$$

$$h_b(x,t;u,v) = \begin{cases} -\frac{1}{\sqrt{2\pi\delta}} e^{\frac{u}{\delta^2}}, & if\ u = (v\tan(\theta(x,y)) - \frac{H}{2\cos(\theta(x,y))}), v \in \Omega \\ \frac{1}{\sqrt{2\pi\delta}} e^{\frac{u}{\delta^2}}, if\ u = (v\tan(\theta(x,y))), v \in \Omega \\ 0, otherwise \end{cases}$$

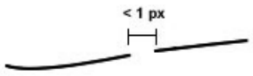
θ(x,y): arah kemiringan dari koordinat (x,y) yang didapat dari tahap estimasi.

Jika *graylevel* bernilai lebih dari nilai *threshold* T yang telah ditentukan, maka titik tersebut dianggap sebagai *ridge*.

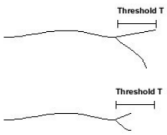
Proses kemudian dilanjutkan dengan tahap pembentukan tulang (*skeletoning / thinning*) dengan *ridge* yang ditandai dengan r(i, j). Tahap ini memiliki beberapa aturan yaitu:

1. Pixel r(i,j) memiliki 2-6 tetangga pixel *ridge*
2. Perubahan pixel tetangga antara pixel gambar latar dan objek pixel *ridge* bernilai 1 dan terletak disekeliling r(i,j)
3. Perkalian pixel tetangga atas, kanan, dan bawah bernilai 0
4. Perkalian pixel tetangga kanan, bawah, dan kiri bernilai 0
5. Pixel ditandai apabila memenuhi aturan 1 hingga 4.
6. Pixel yang telah ditandai dihapus
7. Proses 1 hingga 6 dilakukan Kembali, namun terdapat perubahan pada proses 3 dan 4. Pada proses 3, pixel tetangga yang dihitung adalah kiri, atas, dan kanan, sedangkan pada proses 4 pixel tetangga yang dihitung adalah kanan, bawah, dan kiri. Semua tahapan kemudian diulang hingga taka da lagi pixel yang diberi tangga

Setelah *skeletoning*, tahap terakhir adalah pendeteksian *minutiae* yang dilakuka melalui konvolusi 8 tetangga dengan mencari akhir dan percabangan dari sebuah ridge. Berikut adalah contoh visualisasi dari *ridge ending* dan *ridge bifurcation* (percabangan).

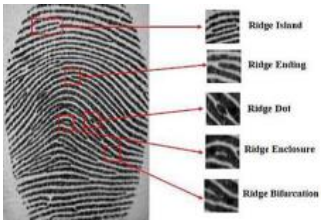


Gambar 5. *Minutiae ridge ending*



Gambar 6. *minutiae bifurcation*

Berikut adalah contoh visualisasi dari *minutiae* pada sidik jari manusia.



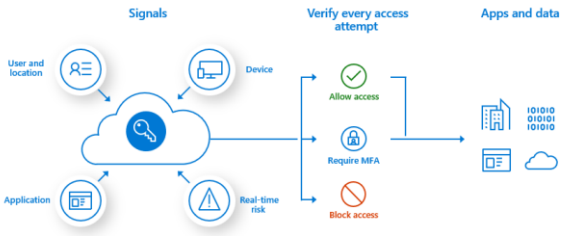
Gambar 7. Ekstraksi sidik jari berdasarkan *minutiae*

Sumber: https://www.bayometric.com/minutiae-based-extraction-fingerprint-recognition/, diakses 9 Desember 2022

Visualisasi ekstraksi sidik jari berdasarkan *minutiae* (gambar 5) menunjukkan dengan jelas bahwa kompleksitas yang dibentuk oleh metode autentikasi dengan sidik jari sangat tinggi. Berdasarkan percobaan yang dilakukan oleh Galton, peluang ditemukannya dua sidik jari yang sama adalah sebesar $1{,}45 \times 10^{-11}$. Nilai otentiknya yang tinggi membuat metode sidik jari menjadi salah satu metode kredensial yang penggunaannya sangat popular karena tergolong lebih aman dan sulit untuk diretas ketimbang metode-metode lainnnya.

MFA DALAM PENGECEKAN AKTIVITAS

Meskipun tingkat keamanan yang dihasilkan melalui metode MFA sudah tergolong tinggi karena kompleksitas dan peluang untuk membobol yang kecil, namun kasus pembobolan masih sering terjadi. Maka dari itu, MFA dikembangkan dan kini terhubung dengan Cloud sehingga dapat melakukan validasi terhadap kecenderungan aktivitas penggunanya. Apabila ditemukan aktivitas yang janggal, maka sistem akan melakukan validasi pada pengguna untuk memastikan bahwa aktivitas tersebut merupakan suatu aktivitas yang memang dilakukan oleh pengguna dan bukan merupakan aksi peretasan. Terkadang, sistem ini juga dihubungkan dengan sistem pemutusan akses otomatis sehingga aktivitas janggal yang dapat menjadi ancaman akan segera dibatalkan. Salah satu contoh sederhana yang sering kita jumpai adalah pada verifikasi ketika kita melakukan *login e-mail* pada perangkat yang belum pernah digunakan untuk mengakses *e-mail* tersebut sebelumnya. Dengan demikian, maka risiko untuk seseorang mengalami peretasan *e-mail* menjadi lebih kecil.



Gambar 8. MFA Overview

Sumber: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

Seperti yang kita ketahui, MFA terdiri atas berbagai lapisan keamanan dengan kompleksitas yang tinggi dan peluang untuk dibobol yang rendah. Walau demikian, aksi peretasan akan tetap berjalan lancer apabila peretas berperan sebagai *Man in the Middle* atau melakukan *Keylogging*, karena semua data korban bahkan autentikasi biometrik yang kamanannya sangat tinggi pun akan terekam. Oleh karena itu, saat ini MFA terus dikembangkan dan telah dihubungkan

dengan *Cloud* sehingga dapat berinteraksi dengan sumber data pengguna.

Jika dikaitkan dengan kasus yang belum lama ini sedang hangat menjadi perbincangan, yaitu peretasan aplikasi perbankan karena kesalahan membuka *link*, maka penggunaan MFA yang dikaitkan dengan *Cloud* sehingga mampu mendeteksi kejanggalan aktivitas pengguna akan sangat berguna. Umumnya, perangkat lunak yang baik akan menampilkan pesan berupa *pop-up message* yang mengingatkan pengguna bahwa *link* yang hendak dibuka merupakan sesuatu yang keamanannya belum tervalidasi dan bertanya kembali pada pengguna apakah ia tetap ingin membuka situs tersebut. Dengan demikian, seluruh pengguna diharapkan untuk lebih berhati-hati dalam mengakses sesuatu. Harapan ini tentunya tidak akan terwujud apabila pengguna tetap gegabah dan mengabaikan pesan tersebut, karena semua balik lagi pada keputusan masing-masing pengguna.

IV. SIMPULAN

MFA atau yang dikenal sebagai *Multi Factor Authentication* memiliki tingkat keamanan yang lebih tinggi ketimbang dengan metode-metode lainnya. Jika dilakukan analisis dari segi kombinatorial, maka hamper tidak mungkin bagi seseorang untuk melakukan peretasan apalagi dengan adanya pembatasan percobaan *login* yang diterapkan. Selain itu, dihubungkannya MFA pada sistem *Cloud* juga semakin memperkuat keamanan karena dapat menginformasikan ancaman pada pengguna. Walau demikian, kewaspadaan setiap pengguna tetap menjadi hal sangat penting yang harus terpenuhi karena sistem tidak sepenuhnya menjamin keamanan data sensitif apabila penggunanya sendiri masih gegabah dalam bertindak

V. UCAPAN TERIMA KASIH

Pertama-tama, penulis ingin mengucap syukur pada Tuhan Yang Maha Esa atas berkat dan kelancaran yang diberikan dalam menulis makalah ini. Selain itu, penulis juga ingin berterima kasih kepada orangtua dan keluarga penulis yang telah memberi dukungan dalama bentuk doa dan material sehingga melancarkan penulisan makalah ini juga. Tidak lupa, penulis tentu ingin berterima kasih kepada dosen IF2120 Matematika Diskrit, yaitu Dr. Fariska Zakhralativa Ruskanda, Dr. Ir. Rinaldi Munir, dan Dr. Nur Ulfa Maulidevi yang sudah mengampu pengajaran terkait Matematika Diskrit, terlebih dalam materi kombinatorial. Terakhir, penulis juga ingin berterima kasih pada teman-teman Teknik Informatika yang telah mendukung pembuatan makalah ini melalui doa dan kata-kata.

REFERENSI

[1] Munir Rinaldi, Kombinatorial(Bagian 1). Bandung, Jawa Barat, 2022., https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Kombinatorial-2020-Bagian1.pdf, diakses 8 Desember 2022

[2] Munir Rinaldi, Kombinatorial(Bagian 2). Bandung, Jawa Barat, 2022, https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Kombinatorial-2020-Bagian2.pdf, diakses 8 Desember 2022

[3] https://glair.ai/blog-posts-id/cara-kerja-multi-factor-authentication, diakses 8 Desember 2022

[4] https://ejournal.ikado.ac.id/index.php/teknika/article/download/5/5/#:~:text=Minutiae%20based%20matching%20adalah%20metode,dari%20dua%20buah%20sidik%20jari., diakses 8 Desember 2022

[5] https://attorneyatlawmagazine.com/latest-articles/various-types-fingerprints, diakses 8 Desember 2022

[6] https://rifqimulyawan.com/blog/pengertian-mfa/, diakses 8 Desember 2022

[7] https://www.studocu.com/id/document/universitas-lambung-mangkurat/matematika-diskrit/kombinatorial-prinsip-penjumlahan-perkalian-teorema-multinomial/37513754, diakses 8 Desember 2022

[8] https://www.logique.co.id/blog/2020/09/10/keyloggers-hacking/, diakses 8 Desember 2022

[9] https://nordvpn.com/id/blog/apa-itu-mitm-attack/#:~:text=Man%20in%20the%20Middle%20Attack%20adalah%20istilah%20peretas%20ketika%20seseorang,antara%20komunikasi%20user%20dan%20website., diakses 8 Desember 2022

[10] https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661, diakses 8 Desember 2022

[11] Hoglund, Greg, and James Butler. Rootkits (2006); subverting the Windows kernel. Addison-Wesley Professional, (2006)., diakkses 9 Desember 2022

[12] Adhikary N., Shrivastava R., Kumar A., Verma S. K., Bag M. and Singh V. (2012); Battering Keyloggers and Screen Recording Software by Fabricating Passwords I. J. Computer Network and Information Security 2012 (pp. 13-21), diakses 9 Desember 2022

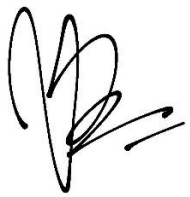
[13] https://www.cloudmatika.co.id/blog-detail/apa-itu-malware, diakses 9 Desember 2022

[14] https://www.cloudmatika.co.id/blog-detail/apa-itu-malware, diakses 9 Desember 2022

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 9 Desember 2020



Vanessa Rebecca Wiyono
13521151