BAB II

TINJAUAN PUSTAKA

2.1.Graphical Password

Graphical password adalah sebuah metode yang di ajukan sebagai alternatif dari password berbasis teks, karena manusia bisa mengingat gambar lebih baik dibandingkan dengan teks [11]. Terdapat dua buah teknik autentikasi dengan menggunakan *graphical password,* yaitu *Recognition Based Technique* dan *Recall Based Technique.* Cara *Recognition Based Technique* melakukan autentikasi adalah dengan memberikan sebuah gambar yang sudah ditentukan ke pengguna dan pengguna diminta untuk memilih urutan dari gambar yang sudah ditentukan. Penggunaan teknik *Recognition Based Technique* sendiri memiliki tingkat keberhasilan sebesar 90%.

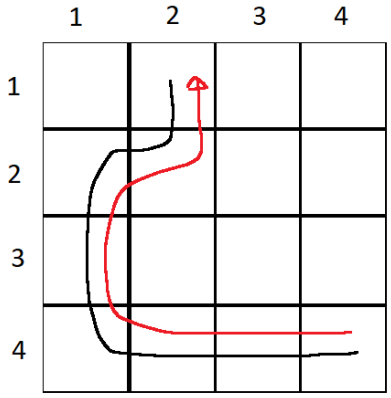
Berbeda dengan *Recognition Based Technique, Recall Based Technique* melakukan autentikasi berdasarkan sesuatu yang digambar oleh pengguna. Pengguna diminta untuk menggambar dan ketika ingin melakukan *sign in*, pengguna diminta untuk menggambar ulang password yang sudah dibuat. Beberapa aplikasi yang menggunakan *Recall Based Technique* adalah Draw a Secret [12] dan Background Draw a Secret [13].

Namun penggunaan graphical password sendiri masih belum sering digunakan dalam aplikasi nyata karena terdapat beberapa kelemahan yang dimiliki oleh graphical password sendiri seperti proses untuk *sign in* yang cukup lama ketika menggunakan salah satu metode graphical password, dimana menurut penelitian yang dilakukan oleh Hartanto,waktu yang diperlukan untuk memasukkan Graphical Password memerlukan waktu 8 kali lebih lama dibandingkan dengan password konvensional [14] dan panjang password yang relatif pendek jika menggunakan teknik autentikasi *Recognition Based Technique* [15] dan berdasarkan hasil survey yang dilakukan oleh Vorster, sebanyak 52% responden tidak mendukung jika perusahaan terkait responden mengimplementasikan *graphical password* dan 57% responden tidak setuju menggunakan *graphical password* sebagai metode

keamanan pada bidang *financial*. Kelemahan dan kurangnya dukungan dari pengguna membuat graphical password kurang dipakai dan diminati pada saat ini.

2.2.State of the Art

Terdapat beberapa penelitian terdahulu mengenai *graphical password*. "Draw a Secret" (DAS) yang dibuat pada tahun 1999 merupakan sebuah sistem keamanan yang menggunakan gambar, dimana pengguna menggambar dalam grid berukuran N x N [12]. Motivasi dari pembuatan sistem DAS sendiri adalah untuk membuat sebuah metode autentikasi yang baru sebagai alternatif dari sistem-sistem keamanan yang ada. Hardware yang menjadi tujuan implementasi utama dari sistem ini adalah berupa Personal Data Assistant (PDA), dimana PDA menggunakan stylus sebagai metode input utamanya dan pengguna bisa menggambar dengan mudah dengan menggunakan stylus. Cara kerja dari DAS sendiri adalah dengan menyimpan koordinat yang dilewati oleh pengguna ketika menggambar grafik, contoh dari input DAS terdapat pada gambar 2.1.



Gambar 2.1. Contoh input DAS

Gambar 2.1 menunjukkan contoh input dari sistem DAS, dimana garis hitam menunjukkan input dari pengguna ketika menggunakan DAS dan garis merah dengan panah menunjukkan arah pengguna menggambar. Data yang disimpan berdasarkan gambar 1 adalah (4,4), (4,3), (4,2), (4,1), (3,1), (2,1), (2,2), (1,2), (5,5). Delapan koordinat pertama menunjukkan arah dari gambar yang dibuat dari pengguna dan koordinat (5,5) menunjukkan stylus yang diangkat. Kelemahan utama yang terdapat dalam sistem DAS adalah jika terdapat gambar garis yang

dekat dengan grid yang disediakan, untuk mengatasi kelemahan tersebut maka sistem DAS akan menolak input pengguna ketika terdapat gambar yang teralu dekat dengan grid yang disediakan [12].

Terdapat juga pengembangan dari DAS, yaitu "Background Draw a Secret" (BDAS), dimana terdapat gambar latar ditambahakan ke dalam DAS untuk mempermudah pengguna mengingat gambar yang sudah dibuat sebagai sistem keamanan [13]. Hasil yang didapatkan ketika menggunakan BDAS adalah gambar yang dibuat oleh pengguna relatif lebih kompleks dibandingkan dengan DAS, kompleks dalam konteks ini adalah terdapat lebih banyak garis yang dibuat memiliki garis yang lebih panjang dan ingatan dari pengguna ketika menggunakan BDAS sama dengan DAS, dimana 95% dari pengguna yang menggunakan BDAS dan DAS ingat dengan gambar yang dibuat sebagai sistem keamanan. Hal tersebut membuat BDAS lebih baik dibandingkan dengan DAS, karena BDAS bisa membuat pengguna menggambar sesuatu yang lebih kompleks dengan tingkat ingatan yang sama dengan DAS.

Persamaan antara BDAS & DAS dengan metode yang penulis ajukan adalah penggunaan gambar sebagai sistem keamanan utamanya dan perbedaannya terdapat pada algoritma yang digunakan, algoritma yang penulis gunakan adalah berupa Siamese Neural Network dan algoritma yang digunakan oleh BDAS & DAS adalah dengan membandingkan koordinat dari input dengan koordinat yang disimpan oleh BDAS & DAS.

Selain BDAS & DAS, terdapat metode lain yang menggunakan gambar sebagai sistem kemanan utamanya, yaitu Passdoodles yang diusulkan oleh Christopher Varenhorst pada tahun 2004 [16]. Motivasi utama ketika membuat sistem tersebut adalah membuat sebuah sistem autentikasi dengan menggunakan doodle sebagai sistem keamanan utamanya. Hasil akhir dari rancangan sistem Passdoodle adalah sebuah metode autentikasi yang ringan dengan menggunakan doodle. Parameter utama yang disimpan oleh Passdoodle adalah kemiripan antara gambar input dengan gambar yang disimpan dan kecepatan. Pengukuran tingkat kemiripan gambar dilakukan dengan melakukan Gaussian Convolution pada gambar input, dimana gambar akan diberikan efek blur dan diproses. Pengukuran kecepatan pada

Passdoodle berguna untuk mengukur konsistensi kecepatan menggambar pada masing-masing pengguna, dimana terdapat karakteristik yang unik dari masing-masing pengguna, yaitu kecepatan menggambar dari masing-masing pengguna. Tingkat akurasi yang didapatkan dari Passdoodles sendiri adalah sebesar 98.5% ketika menggunakan parameter kecepatan dan kemiripan gambar. Terdapat beberapa kesamaan antara Passdoodle dengan metode yang penulis ajukan, salah satunya adalah penggunaan doodle sebagai input utama dan perbedaannya terdapat pada algoritma yang digunakan, Passdoodle menggunakan Gaussian Convolution dan kecepatan menggambar untuk mengukur kemiripan gambar, sedangkan metode yang penulis ajukan menggunakan Siamese Neural Network untuk membandingkan antara gambar input dengan gambar di *database*.

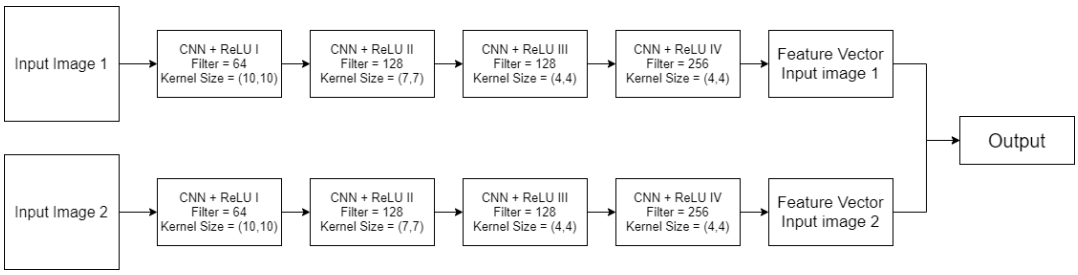
Di tahun 2019, terdapat juga *graphical password* baru yang didesain oleh Asmat, et al bernama Conundrum-Pass [17]. Motivasi dari pembuatan Conundrum-Pass sendiri adalah sebagai metode baru dari *graphical password* dan untuk mengurangi serangan-serangan yang terjadi di dalam *graphical password* seperti *dictionary attack, shoulder surfing* atau *eavesdropping.* Terdapat empat proses dari Conundrum-Pass sendiri, yaitu *picture selection, picture division, pattern generation, grid shuffling.* Dalam proses *Picture Selection* pengguna diminta untuk memilih gambar yang ingin dipakai di dalam *lock screen* pengguna. Setelah pengguna memilih gambar, pengguna diminta untuk memilih jumlah matriks untuk memisahkan gambar. Ukuran matriks yang harus pengguna pilih antara 2-4 dan gambar akan dipisahkan dengan menggunakan algoritma picture_Division(). Setelah gambar dipisahkan, dalam proses *pattern generation* pengguna diminta untuk memilih pola dari gambar yang sudah dipecah di proses sebelumnya dan pola yang sudah terpilih akan disimpan di dalam *database*. Proses *grid shuffling* berjalan ketika pengguna ingin memasukkan password yang sudah dibuat. Potongan gambar akan diacak dan pengguna akan menginput pola yang sudah dibuat di proses sebelumnya.

Hasil yang didapatkan dari penelitian oleh Asmat, et al dilakukan secara kualitatif, dimana penulis memberikan kuesioner di akhir penelitian untuk mengukur kepuasan dari penggunaan Conundrum-Pass, tingkat kepercayaan dari pengguna ketika menggunakan aplikasi dan kelayakan untuk digunakan di dalam

industri. Kebanyakan dari partisipan yang mengikuti eksperimen tersebut puas ketika menggunakan Conundrum pass, dan 70% dari partisipan mengatakan percaya untuk menggunakan aplikasi dan 60% partisipan mengatakan bahwa aplikasi layak untuk di deploy ke dalam industri.

2.3. Siamese Neural Network

Siamese Neural Network adalah sebuah algoritma untuk melakukan Image Recognition [10]. Siamese Neural Network sendiri dibuat untuk mengurangi jumlah dataset dari algoritma Image Recognition, karena dataset yang banyak untuk melakukan training sendiri memerlukan *resource* yang lebih. Model yang dimiliki oleh Siamese Neural Network sendiri merupakan dua buah Network yang merupakan penggabungan dari beberapa Convolutional Neural Network (CNN) dan menggunakan Recified Linear Unit (ReLU) untuk menghasilkan dua buah feature map untuk masing-masing input, pada Sistem "Passwle" masing-masing Neural Network memiliki 4 pasang CNN dan ReLU. Filter CNN yang digunakan pada keempat buah CNN tersebut adalah sebesar 64, 128 dan 256, sedangkan besar kernel yang digunakan adalah sebesar (10,10), (7,7) dan (4,4). Feature map yang sudah dibentuk pada akhir model akan diubah menjadi sebuah feature vector. Kemudian, dua buah feature vector yang sudah didapatkan akan dibandingkan jaraknya sehingga menghasilkan sebuah output yang memperhitungkan tingkat kemiripan dari kedua buah input. Gambar 2.2 menunjukkan ilustrasi model dari Siamese Neural Network.



Gambar 2.2. Model Siamese Neural Network

Untuk menguji tingkat akurasi algoritma, Siamese Neural Network menggunakan Omniglot dataset sebagai dataset utamanya. Omniglot dataset berisikan karakter-karakter dari bahasa Korea, Latin, Sansekerta hingga bahasa yang digunakan di dunia fiksi seperti Klingon dan Aurek-Besh. Hasil yang didapatkan berdasarkan pengujian dengan menggunakan Omniglot dataset adalah diatas 90%. Terdapat beberapa aplikasi dari algoritma Siamese Neural Network, seperti SigNet yang digunakan untuk mendeteksi tandatangan palsu secara offline [18], mendeteksi penulis dari tulisan tangan [19] dan pendeteksi gaya berjalan pada seseorang untuk *human identification* [20].

Akurasi yang dimiliki oleh Siamese Neural Network jika dilihat dari penelitian [18] relatif lebih bagus dibandingkan dengan algoritma lainnya. SigNet yang menggunakan Siamese Neural Network sebagai algoritmanya mendapatkan akurasi sebesar 100% dan berada di peringkat satu ketika melakukan *signature forgery* dengan menggunakan CEDAR Signature Dataset. SigNet juga memiliki tingkat akurasi yang lebih tinggi dibandingkan dengan algoritma Compact Corelated Features, dimana SigNet mendapatkan akurasi sebesar 77.76 %.

2.4. USE Questionnaire

USE Questionnaire merupakan sekumpulan pertanyaan yang digunakan untuk mengukur faktor *Userfulness, Satisfaction* dan *Ease of Use* [21]. *USE questionnaire* sendiri dibuat oleh Arnold Lund untuk mengetahui penilaian dari pengguna terhadap ketiga metrik yang sudah disebutkan diatas. Pertanyaan-pertanyaan yang digunakan di dalam *USE Questionnaire* terdapat di tabel 2.1.

Penilaian dari USE Questionnaire menggunakan skala 1-7 untuk mengukur nilai dari setiap faktornya, dimana nilai satu menunjukkan bahwa responden sangat tidak setuju akan pernyataan yang diberika, dan nilai tujuh menunjukkan bahwa responden sangat setuju akan pernyataan yang diberikan. Pemakaian *USE Questionnaire* juga bisa disesuaikan dengan memilih beberapa pertanyaan dari setiap faktor. Belum terdapat penggunaan USE Questionnaire untuk menilai penelitian graphical password lainnya.

No.	Pertanyaan
Userfulness	
1	It helps me be more effective.
2	It helps me be more productive.
3	It is useful.
4	It gives me more control over the activities in my life.
5	It makes the things I want to accomplish easier to get done.
6	It saves me time when I use it.
7	It meets my needs.
8	It does everything I would expect it to do.
Ease of Use	
9	It is easy to use.
10	It is simple to use.
11	It is user friendly.
12	It requires the fewest steps possible to accomplish what I want to do with it.
13	It is flexible.
14	Using it is effortless.
15	I can use it without written instructions.
16	I don't notice any inconsistencies as I use it.
17	Both occasional and regular users would like it.
18	I can recover from mistakes quickly and easily.
19	I can use it successfully every time.
Ease of Learning	
20	I learned to use it quickly.
21	I easily remember how to use it.
22	It is easy to learn to use it.
23	I quickly became skillful with it.
Satisfaction	
24	I am satisfied with it.
25	I would recommend it to a friend.
26	It is fun to use.

27	It works the way I want it to work.
28	It is wonderful.
29	I feel I need to have it.
30	It is pleasant to use.

Tabel 2.1. Pertanyaan *USE Questionnaire*

2.5. MD5 *Hash* Algorithm

MD5 merupakan sebuah algoritma *hash* yang dibuat pada tahun 1992 oleh Ronal Linn Rivest [22]. Hasil dari algoritma MD5 sendiri adalah berupa sebuah string dengan 128-bit dari input yang diberikan. Aplikasi dari MD5 sendiri bisa digunakan untuk menyembunyikan password atau username dalam sebuah website agar penyerang tidak bisa melihat password secara langsung. Metode penyerangan utama dalam algoritma *hash* MD5 adalah dengan menggunakan Dictionary Attack dan Rainbow Table [23].

Cara penyerangan dengan metode Dictionary Attack adalah dengan menyimpan banyak hasil *hashing* dari berbagai string dan menyimpannya di dalam sebuah *database*. Keberhasilan Dictionary Attack sendiri bergantung kepada jumlah string dan hasil *hash* yang disimpan di dalam *database* yang penyerang gunakan. Cara penyerangan dengan menggunakan metode Rainbow Table adalah dengan menggunakan fungsi reduksi untuk mengubah hasil *hashing* menjadi plain text. Fungsi reduksi dipakai secara berulang hingga ditemukan password di dalam *hash* tersebut.

Untuk mencegah penyerangan, terdapat beberapa countermeasure yang bisa digunakan, seperti menggunakan salt untuk mencegah ditemukannya hasil *hashing* di dalam *database* pada Dictionary Attack dan mencegah Rainbow Table untuk meretas hasil *hash* MD5.