PENGAWALAN KAEDAH PENGESAHAN DALAM PERBANKAN INTERNET MENGGUNAKAN KAEDAH PENYULITAN MADU

NIK FATHIRA W. BAHARUDDIN
RAVIE CHANDREN A/L MUNIYANDI

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Kebanyakan pengguna akaun secara atas talian menggunakan kata laluan yang lemah dan senang untuk diteka. Kata laluan ini disimpan di dalam pangkalan data setelah dilakukan penyulitan. Namun begitu, terdapat pelbagai cara untuk menyahsulit kata laluan tersebut terutamanya kata laluan yang lemah. Hal ini akan menjejaskan keselamatan pengguna sesebuah akaun. Oleh itu, objektif yang diketengahkan adalah untuk membantu pengguna yang menggunakan kata laluan yang lemah daripada serangan daya kasar menggunakan kaedah penyulitan madu (*Honey Encryption).* Apabila berlaku serangan daya kasar, penyulitan madu akan menghasilkan data-data yang menyerupai data sebenar. Data-data tersebut akan mengelirukan penggodam kerana tidak dapat membezakan data sebenar dengan data palsu.

1 PENGENALAN

Kecanggihan teknologi pada masa kini telah menyumbang kepada banyak industri termasuklah industri perbankan. Kini aktiviti perbankan seperti menyemak baki akaun, memindahkan wang di antara akaun, membuat bayaran dan lain-lain boleh dilakukan secara atas talian. Perbankan internet ini boleh dilakukan dari mana-mana sahaja di seluruh dunia selagi mempunyai komputer atau telefon pintar bersama dengan capaian internet. Namun begitu, terdapat orang-orang yang tidak bertanggungjawab yang menggunakan kesempatan ini untuk melakukan jenayah siber seperti mengakses akaun secara tidak sah untuk mengaut keuntungan secara haram. Oleh yang demikian, keselamatan pengguna dalam menggunakan perbankan internet terjejas.

2 PENYATAAN MASALAH

Semestinya setiap bank yang menawarkan perbankan internet akan memastikan keselamatan pengguna dalam menjalankan urusan perbankan secara atas talian. Pelbagai teknologi

keselamatan digunakan seperti pemasangan sistem untuk mengesan penceroboh, dinding keselamatan, log keluar automatik dan banyak lagi. Namun, risiko keselamatan tetap ada bagi penggunaan perbankan internet kerana terdapat penggodam yang turut pakar dalam bidang tersebut. Mereka akan berjaya untuk mengakses akaun pengguna dengan memecahkan sesebuah kata laluan.

Salah satu cara yang digunakan untuk memecahkan kata laluan tersebut ialah melalui serangan daya kasar. Serangan daya kasar akan mencuba kesemua kombinasi huruf, nombor dan karakter sehingga menjumpai kombinasi yang tepat. Serangan daya kasar boleh memakan masa yang lama bergantung kepada kesulitan sesuatu kata laluan. Secara teorinya, daya kasar mampu memecahkan apa jua kata laluan seperti Blowfish, AES, DES, Triple DES dan sebagainya. Hal ini amat memudaratkan dari segi keselamatan sesebuah akaun. Tambahan lagi, ramai yang menggunakan kata laluan yang mudah. (Krisnaldi Eka Pramudita, n.d.)

Berdasarkan (Noorunnisa & Afreen, 2016), 10 kata laluan yang sering digunakan ialah 123456, 12345, 123456789, kata laluan, iloveyou, princess, rockyou, 12345678, abc123. Ini akan memudahkan penggodam untuk meneka kata laluan yang digunakan oleh sesebuah akaun.

3 OBJEKTIF KAJIAN

Projek ini bertujuan untuk membangunkan kaedah pengesahan yang selamat kepada pengguna perbankan internet menggunakan penyulitan madu. Secara umumnya penyulitan madu mampu untuk melawan serangan daya kasar dengan menghasilkan data-data yang tidak boleh dikawal oleh serangan daya kasar. Konsep ini dapat meningkatkan keselamatan pengguna akaun yang hanya menggunakan kata laluan yang lemah.

4 METOD KAJIAN

Penggunaan model pembangunan yang sesuai penting untuk memastikan perjalanan projek berjalan dengan lancar dan menjamin hasil kerja yang berkualiti. Kaedah pengesahan masuk

sesebuah akaun menggunakan penyulitan madu melibatkan beberapa fasa pembangunan dan ditambah dengan penggunaan perisian dan perkakasan yang bersesuaian. Kaedah ini dibangunkan oleh Ari Juels yang pada sebelumnya merupakan ketua saintis dari RSA (Noorunnisa & Afreen, 2016). Fasa pembangunan termasuk fasa perancangan, analisis, reka bentuk, pengujian dan dokumentasi. Kaedah ini dapat membantu pengguna yang menggunakan kata laluan yang mudah.

4.1 Fasa Perancangan

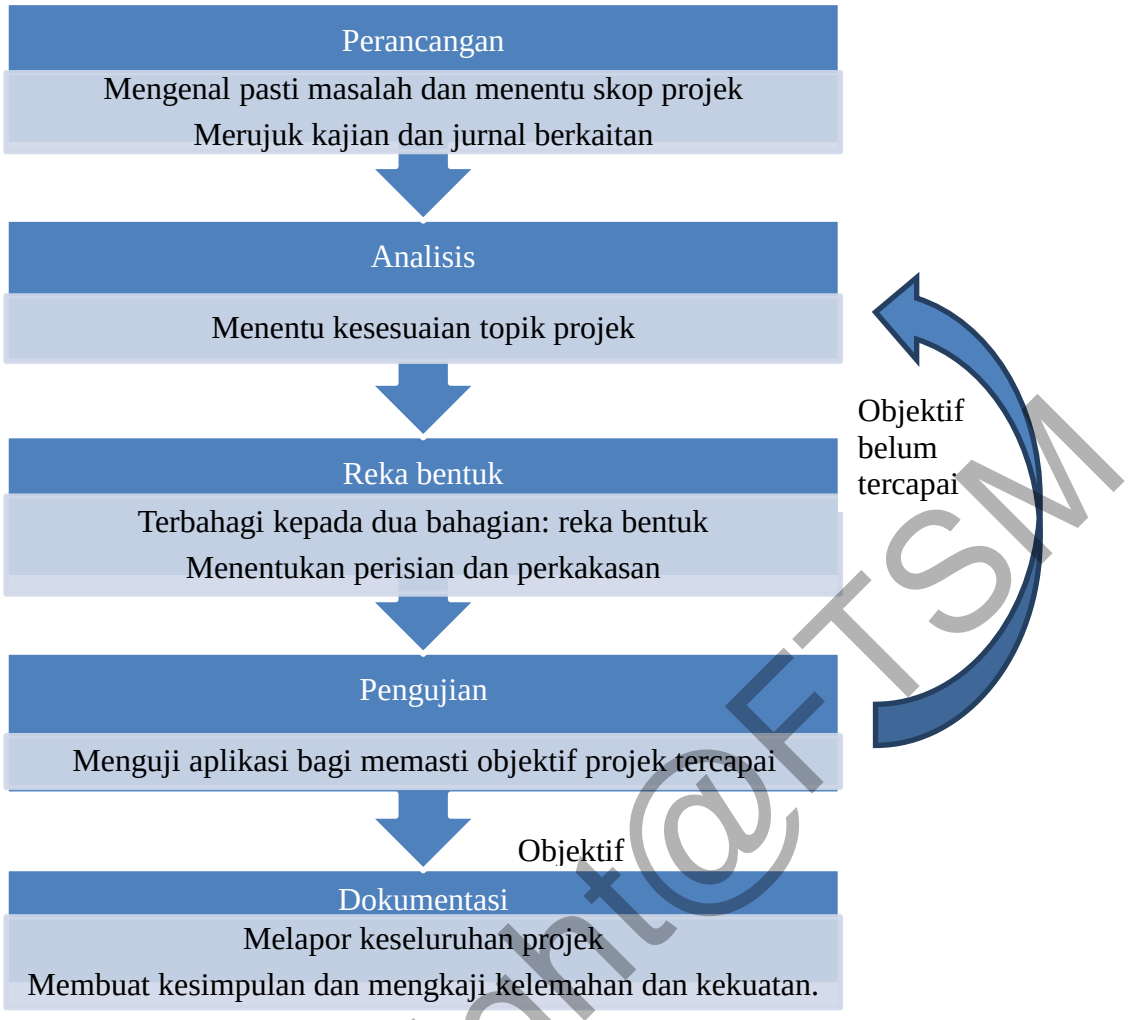
Fasa ini melibatkan proses pengenalpastian masalah, objektif, persoalan kajian dan menentukan skop. Langkah seterusnya adalah sorotan susastera yang melibatkan pengumpulan, pencarian dan pembacaan jurnal dan kajian lepas bagi mencetus idea dan inspirasi. Contoh topik yang berkaitan dikaji terutama berkaitan dengan konsep penyulitan madu itu sendiri dari segi cara pembangunannya. Penggunaan internet untuk mencapai maklumat berkaitan dilakukan. Maklumat dikumpul, distruktur dan disintesis dan dipersembah secara kritis dan kreatif dalam fasa analisis.

4.2 Fasa Analisis

Fasa ini melibatkan analisis dan tafsiran maklumat yang dikumpul dalam fasa perancangan. Analisis tentang kesesuaian topik dan menilai kepentingan untuk menjalankan kajian ini dilakukan. Selain daripada itu, analisis tentang perkakasan dan perisian juga dijalankan untuk memasti perkakasan dan persisian yang sedia ada adalah sesuai untuk membangun projek ini.

4.3 Fasa Reka Bentuk

Fasa ini merupakan fasa yang penting dalam mengguna pelbagai perisian. PHP atau *Hypertext Preprocesser* digunakan bagi menghasilkan reka bentuk antara muka dan sistem manakala PHP MyAdmin digunakan sebagai pelayan pangkalan data untuk menyimpan kata laluan dan *honeywords* bagi pengguna. Bahasa pengaturcaraan Python turut digunakan bagi menghasilkan *honeywords* bagi setiap pengguna akaun.



Rajah 4.1: Gambar rajah perancangan reka bentuk

4.4 Fasa Pengujian

Fasa ini bertujuan untuk menentukan sama ada sistem yang dibangunkan telah mencapai objektif yang telah ditetapkan pada bab-bab semasa membangunkan sistem. Pengujian ini juga bertujuan untuk mengenalpasti kelemahan sistem bagi mencari jalan penyelesaian untuk mengatasi kelemahan tersebut. Penghasilan *honeywords* bagi setiap pengguna akaun yang berdaftar diuji. *Honeywords* yang dihasilkan mestilah secara rawak dan berlainan bagi setiap pengguna. Ini adalah untuk memastikan *honeywords* yang dihasilkan kelihatan meyakinkan dan akan mengelirukan penggodam yang menyerang sesebuah akaun.

Perkakasan dan perisian yang diguna untuk membangun projek harus dipilih dengan teliti. Perkakasan dan perisian yang baik berfungsi dengan lancar serta menyokong pembangunan sistem.

Jadual 4.1 Jadual Perkakasan

Perkakasan	Spesifikasi Perkakasan
Model	Asus A550C
Sistem Operasi	Windows 8
Pemproses	Intel Core i3-3217U. CPU @ 1.8 GHz
Memori (RAM)	4.00 GB
Kad Grafik	NVIDIA GEFORCE Graphics
Pelayar	Google Chrome, Mozilla Firefox
Perkakasan Input	Papan Kekunci, Tetikus

Spesifikasi keperluan perisian yang diguna untuk membangun ini harus dapat menghasilkan sistem yang baik dan dapat memberi ciri-ciri keselamatan.

5 HASIL KAJIAN

Bahagian ini membincang hasil daripada proses pembangunan pengawalan kaedah pengesahan. Penerangan yang mendalam tentang reka bentuk dan fungsi sistem diperihal. Fasa reka bentuk adalah fasa yang penting dalam pembangunan projek. Dalam projek ini, Python digunakan untuk menghasilkan algoritma bagi menghasilkan *honeywords* yang merupakan kata laluan palsu. *Honeywords* disimpan didalam pangkalan data bersama kata laluan pengguna yang sebenar. Penggunaan PHP atau *Hypertext Preprocesser* adalah untuk menghasilkan sistem dan antara muka bagi projek ini. PHP MyAdmin turut digunakan sebagai pelayan pangkalan data bagi menyimpan data.

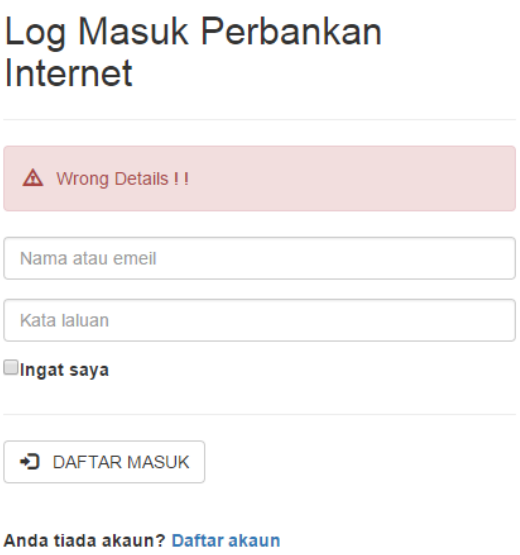
Rajah dibawah menunjukkan gambaran tentang reka bentuk antara muka bagi sistem perbankan internet.

Rajah 5.1: Gambar rajah antara muka untuk log masuk.

Gambar rajah ini dipaparkan apabila pengguna ingin log masuk ke sesebuah akaun perbankan internet. Pengguna perlu memasukkan nama dan kata laluan yang berdaftar untuk mengakses sesebuah akaun.

Rajah 5.2: Gambar rajah antara muka bagi laman utama.

Apabila pengguna berjaya log masuk ke sesebuah akaun, laman utama perbankan internet dipaparkan.



Rajah 5.3: Gambar rajah antara muka bagi akaun yang menerima data yang salah.

Akaun akan memberi amaran automatik apabila dimasukkan data *honeywords* berlaku demi keselamatan pengguna akaun.

6 KESIMPULAN

Sistem pengawalan kaedah pengesahan ini dijangka dapat membantu meningkatkan ciri-ciri keselamatan dalam melakukan transaksi atas talian terutamanya perbankan internet. Hal ini amat penting dalam menjaga privasi data-data sulit. Data sulit ini perlu dijaga kerana ia dapat menjejaskan keselamatan seseorang jika jatuh ke tangan orang yang salah.

Pengawalan kaedah pengesahan masuk ini akan membantu pengguna akaun yang masih mengamalkan penggunaan kata laluan yang lemah. Dengan adanya penggunaan algoritma madu, akaun pengguna dapat mengelakkan diceroboh oleh penggodam yang melakukan serangan daya kasar terhadap akaun tersebut.

7 RUJUKAN

Noorunnisa, N. S., & Afreen, K. R. (2016). Review on Honey Encryption Technique, 5(2), 2014–2017.

Tyagi, N., Wang, J., Wen, K., & Zuo, D. (2015). Honey Encryption Applications Implementation of an encryption scheme resilient to brute-force attacks.

Juels, A., & Ristenpart, T. (2014). Honey Encryption: Security Beyond the Brute-Force Bound.

Ji Won Yoon, Hyoungshick Kim, Hyun-Ju Jo, Hyelim Lee, K. L. (n.d.). Visual Honey Encryption: Application to Steganography.

D. Florencio and C. Herley. (2007). A large-scale study of web password habits.

Honeyball Jon. (2011). How a cheap graphics card could crack your password in under a second | Alphr. Retrieved December 20, 2016, from http://www.alphr.com/blogs/2011/06/01/how-a-cheap-graphics-card-could-crack-your- password -in-under-a-second

Krisnaldi Eka Pramudita. (n.d.). Brute Force Attack dan Penerapannya pada Password Cracking.