JURNAL TIMES
TECHNOLOGY INFORMATICS & COMPUTER SYSTEM

Volume IX No 1, Juni 2020
*p*ISSN : 2337 – 3601
*e*ISSN : 2549 – 015X

Tersedia *online* di http://ejournal.stmik-time.ac.id

VERIFIKASI USERNAME/PASSWORD MENGGUNAKAN KEYSTROKE DYNAMICS

Edi
Department of Information System
STMIK TIME
Jalan Merbabu No. 32 AA-BB, Medan, North Sumatra 20212, Indonesia
e-mail: edi_foe@yahoo.com

Abstrak
Password bisa disebut sebagai milik pribadi yang paling berharga, karena *password* memegang peranan dalam kehidupan sehari-hari, seperti pada saat menggunakan ATM, mengakses *e-mail*, dan sebagainya. Begitu pentingnya *password*, sehingga apabila *password* diketahui oleh orang lain, maka dapat diperkirakan akibat yang akan terjadi. *Keystroke dynamics* adalah biometrik yang memverifikasi seorang user berdasarkan irama pengetikan. Metode yang dipakai adalah statistik yakni dengan membandingkan pengetikan pada saat *login* dengan profil pengetikan yang tersimpan sebelumnya. Dengan adanya *keystroke dynamics* maka mampu menjamin keamanan data, karena di samping identifikasi yang dilakukan terhadap *password* yang diketik sekaligus juga dilakukan verifikasi terhadap irama pengetikan.
Kata Kunci: *keystroke dynamics*, biometrik, *password*

1. Pendahuluan

Password dapat diibaratkan seperti kunci rumah. Jika kunci anda jatuh ke tangan orang lain, maka ia bisa leluasa masuk rumah. Sebagian orang menyimpan password dalam telepon genggam ataupun menulisnya dalam secarik kertas untuk menghindari kelupaan. Apabila secara tidak sengaja password tersebut jatuh/terlihat oleh orang lain, maka tentu saja ia dapat masuk ke sistem komputer kita.

Oleh karena itu, diperlukan suatu metode yang tepat dalam mengatasi masalah di atas. Metode tersebut harus dapat mengamankan komputer kita dari pengaksesan password oleh illegal user. Metode yang dimaksud adalah keystroke dynamics. Keystroke dynamics merupakan teknik verifikasi identitas diri seseorang berdasarkan irama pengetikan keyboard. Teknologi ini akan memantau setiap pengetikan tombol-tombol keyboard yang dilakukan oleh seorang user. Apabila irama pengetikan yang dilakukan oleh user tidak sama dengan pola pengetikan yang tersimpan dalam database maka user tersebut tidak dapat masuk ke sistem.

Keystroke dynamics adalah suatu biometrik yang didasarkan bahwa setiap orang memiliki perilaku atau karakteristik yang berbeda-beda dalam hal pengetikan. Keystroke dynamics adalah proses menganalisa bagaimana cara seseorang mengetik pada keyboard sehingga dapat diidentifikasi berdasarkan irama pengetikan. Keystroke dynamics juga disebut dengan keyboard dynamics, keystroke analysis, typing biometrics dan typing rhythms.

2. Landasan Teori

Biometrik

Biometrik adalah suatu ukuran, karakteristik fisik atau ciri perilaku pribadi yang digunakan untuk mengenali identitas atau memverifikasi identitas diri sendiri. Karakteristik fisik yang paling menonjol untuk dijadikan sebagai identifikasi biometrik adalah sidik jari, suara, iris mata atau selaput pelangi, raut muka, dan hand geometry (ilmu ukur tangan).

Dengan menentukan karakteristik fisik seseorang yang menonjol dalam suatu pemeriksaan pengesahan dan membandingkan data ini dengan menyimpan acuan biometrik, identifikasi untuk seorang pemakai yang spesifik dapat ditentukan dan pengesahan untuk akses dapat diwarisi.

Sebenarnya teknologi biometrik sudah dikenal sejak zaman Mesir kuno. Rekaman roman muka dan ukuran bagian tubuh yang dikenali biasanya digunakan untuk meyakinkan bahwa yang bersangkutan adalah orang yang sebenarnya. Akses kontrol seperti itulah awal dari workflow sistem pengamanan. Logikanya, tidak seorang pun memiliki akses tanpa ia percaya dan orang lain dilarang. Teknologi akses kontrol berusaha mengotomatisasi proses yang menjawab dua pertanyaan dasar sebelum menawarkan berbagai jenis akses. Yang pertama, “Siapakah Anda?” dan kedua “Apakah Anda benar seperti yang Anda katakan?”. Pertanyaan pertama mewakili fungsi identifikasi, dan pertanyaan kedua mewakili fungsi verifikasi (pembuktian).

Keunggulan dari suatu sistem biometrik ditentukan oleh FAR (False Accept Rate) atau Type I Error dan FRR (False Reject Rate) atau Type II Error. FAR artinya kesalahan di mana biometrik menolak user yang valid sedangkan FRR artinya kesalahan di mana biometrik menerima user yang tidak sah. Sistem biometrik yang unggul diharuskan memiliki FAR 0% dan FRR 0% atau memiliki tingkat error yang kecil.

Keystroke Dynamics

Keystroke dynamics adalah suatu biometrik yang didasarkan bahwa setiap orang memiliki perilaku atau karakteristik yang berbeda-beda dalam hal pengetikan. *Keystroke dynamics* adalah proses menganalisa bagaimana cara seseorang mengetik pada *keyboard* sehingga dapat diidentifikasi berdasarkan irama pengetikan. *Keystroke dynamics* juga disebut dengan *keyboard dynamics*, *keystroke analysis*, *typing biometrics* dan *typing rhythms*.

Akses ke sistem komputer biasanya dikontrol oleh *user account* dengan *username* dan *password*. Ini akan menjadi resiko seandainya *username* dan *password* jatuh ke tangan yang salah. Biometrik lain seperti *fingerprints* bisa digunakan sebagai alternatif penggunaan *username* dan *password* dan merupakan biometrik dengan keamanan kuat, tetapi *fingerprints* memerlukan biaya yang mahal seperti untuk pembelian *hardware*. Tetapi, dengan menggunakan *keystroke dynamics* tidak diperlukan biaya yang mahal seperti *hardware*, karena yang diperlukan cukup *keyboard* dan *software*.

Keystroke dynamics sekaligus dapat digunakan untuk identifikasi maupun verifikasi. Untuk identifikasi, *keystroke dynamics* akan mendeteksi apakah *username* dan *password* yang dimasukkan sudah benar. Untuk verifikasi, *keystroke dynamics* akan mendeteksi apakah *user* yang masuk ke sistem komputer benar-benar adalah *user* sebenarnya berdasarkan irama pengetikan pada *keyboard*.

Keystroke dynamics memasukkan pengukuran-pengukuran yang berbeda yang dapat digunakan untuk mendeteksi pada saat user menekan tombol di *keyboard*. Pengukuran yang dimungkinkan seperti:

- Jarak antara tombol-tombol.
- Durasi dari tombol yang ditekan.
- Frekuensi kesalahan (berapa sering user menggunakan *backspace*).
- Kebiasaan menggunakan tambahan tombol *keyboard*, seperti pada saat memasukkan nomor menggunakan numpad.
- Kecepatan pengetikan.
- Penggunaan dua tombol sekaligus seperti pada saat menuliskan huruf kapital, harus memakai tombol *shift* dengan tombol huruf lainnya.
- Kekuatan yang digunakan untuk menekan tombol pada saat pengetikan (memerlukan *keyboard* khusus).

Banyak faktor yang menjadi pertimbangan mengapa *keystroke dynamics* dapat dijadikan sebagai alternatif sistem keamanan. Beberapa hal penting antara lain:

- Menggabungkan *password* dengan pola pengetikan sehingga menghasilkan *password* yang kuat yang sulit ditembus oleh penyusup.
- Harga murah karena tidak diperlukan tambahan *hardware*, yang diperlukan hanya *keyboard* dan *software*. Jika dibandingkan dengan biometrik lain, maka *keystroke dynamics* dikatakan paling murah dibandingkan dengan biometrik lain yang memerlukan *hardware* yang sangat mahal.
- Dapat diterapkan pada berbagai segi kehidupan yang masih memerlukan *password*, seperti penggunaan ATM, *e-commerce*, dan juga dapat dipakai pada saat *login* ke *server*, maupun dari komputer *client* ke *server* yang membutuhkan *password*.

Di samping mempunyai kelebihan, terdapat juga kelemahan antara lain:

- Memiliki FRR tinggi, sehingga akan membuat jengkel user yang valid tetapi tidak dapat masuk ke dalam sistem.
- Sensitif terhadap pergantian keyboard dan fisik dari user, misalnya jika user sakit atau mengalami kelelahan maka akan berpengaruh terhadap pengetikan keyboard.

Standar Deviasi

[1] dan [2] membandingkan sampel menggunakan rata-rata dan standard deviasi antartombol *keyboard*.

$$s = \sqrt{\frac{\sum(x - \bar{x})^2}{n}}$$

Di mana:

x = selang waktu penekanan tombol maupun selang waktu antartombol *keyboard*

$\bar{x}$ = rata-rata

n = jumlah *login*

s = standar deviasi

Rumusan standar deviasi di atas berarti setiap login sebelumnya perlu disimpan agar standar deviasi dapat dihitung. Dengan mengubah rumus standar deviasi di atas, maka dapat dihasilkan rumusan yang tidak memerlukan semua *login* sebelumnya.

$$s = \sqrt{\frac{\sum x^2}{n} - \left(\frac{\sum x}{n}\right)^2}$$

Rumus standar deviasi yang telah diubah, memungkinkan perhitungan menjadi lebih cepat dan mengurangi kapasitas penyimpanan untuk profil *user*.

Weighted Latencies

Masalah utama dalam menggunakan standar deviasi adalah kemungkinan *digraph* dapat diterima walaupun *digraph* tersebut mempunyai perbedaan waktu yang besar terhadap *digraph* yang disimpan di profil *user*, sehingga konsekuensinya banyak *digrap*h yang akan diterima yang mengakibatkan *FAR* (*False Acceptance Rate*) tinggi.

Cara untuk mengurangi masalah di atas adalah dengan memberikan bobot dalam pembuktian verifikasi. Jika nilai standar deviasi dibandingkan dengan nilai rata-rata adalah besar, maka nilai bobot yang dihasilkan adalah kecil.

$$W = \left(\frac{1}{\sum \left(\frac{\bar{x}}{s} \right)} \times \left(\frac{\bar{x}}{s} \right) \right) \times 100\%$$

di mana:
W = bobot untuk masing-masing tombol
$\bar{x}$ = rata-rata
s = standar deviasi

3. Metode Penelitian

Metode penelitian yang digunakan adalah *waterfall model* menurut D. Avison dan G. Fitgerald [3] adalah sebagai berikut:

- Studi kelayakan, menetapkan hal yang akan disimulasikan, mencari teori pendukung, dan manfaatnya untuk masyarakat.
- Investigasi sistem, mengumpulkan informasi tentang keystroke dynamics.
- Analisis sistem, mengkaji dan menganalisa informasi untuk dirangkum agar lebih efektif serta menganalisa kebutuhan sesuai informasi yang dirangkum.
- Perancangan sistem, merancang algoritma sesuai metode yang digunakan.
- Implementasi, mengimplementasikan algoritma ke dalam perangkat lunak serta menguji sistem hasil implementasi algoritma.

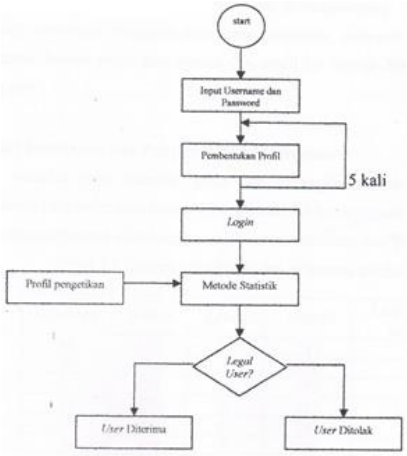
Ada 5 (lima) tahap yang akan dilakukan dalam perangkat lunak Verifikasi Username/Password Menggunakan Keystroke Dynamics, yaitu:

- Proses input username dan password dari user.
- Proses pembentukan profil pengetikan dari user.
- Proses login dari user.
- Proses verifikasi login dari user
- Hasil verifikasi login dari user

4. Hasil Penelitian

Pengimplementasian atau pengujian terhadap perangkat lunak Verifikasi Username/Password Menggunakan Keystroke Dynamics dilakukan dengan bantuan 9 orang user yang masing-masing memiliki irama pengetikan yang berbeda. Hasil implemenasi perangkat lunak ini nantinya akan dijadikan sebagai bahan untuk menghitung FAR (False Acceptance Rate) dan FRR (False Rejected Rate).

Tingkat kecocokan pengetikan pada saat login dengan profil pengetikan yang dilakukan dalam implementasi oleh 9 orang user adalah 80%. Penetapan tingkat kecocokan tersebut dilakukan agar adanya keseragaman di antara user yang melakukan pengujian.



Gambar 1. Tahapan proses perangkat lunak

Pengujian Oleh User

User 1 memasukkan kata 'fujianto' sebagai *username* dan *password*. Berikut adalah hasil *login user* 1:

Tabel 1. Hasil *login user* 1

Login ke-	*Username*			Password			Login
	Kecocokan (%)	Bobot (%)_	Login	Kecocokan (%)	Bobot (%)_	Login	
1	93.33	95.75	Sukses	100	100	Sukses	Sukses
2	73.33	69.91	Gagal	100	100	Sukses	Gagal
3	86.67	79.94	Gagal	100	100	Sukses	Gagal
4	93.33	92.41	Sukses	100	100	Sukses	Sukses
5	93.33	96.95	Sukses	100	100	Sukses	Sukses
6	100	100	Sukses	100	100	Sukses	Sukses
7	86.67	89.82	Sukses	66.67	69.17	Gagal	Gagal
8	100	100	Sukses	86.67	83.50	Sukses	Sukses
9	80	82.06	Sukses	100	100	Sukses	Sukses
10	100	100	Sukses	100	100	Sukses	Sukses

Dari 50 kali *login* yang dilakukan, diperoleh 46 kali *login* yang dinyatakan 'sukses', 48 kali *login* pada *username* yang dinyatakan 'sukses', dan 48 kali *login* pada *password* yang dinyatakan 'sukses'.

User 2 memasukkan kata 'manipulasi' sebagai *username* dan *password*. Dari 50 kali *login* yang dilakukan, diperoleh 24 kali *login* yang dinyatakan 'sukses', 30 kali *login* pada *username* yang dinyatakan 'sukses', dan 39 kali *login* pada *password* yang dinyatakan 'sukses'.

User 3 memasukkan kata 'komputer' sebagai *username* dan *password*. Dari 50 kali *login*, diperoleh 46 kali *login* yang dinyatakan 'sukses', 48 kali *login* pada *username* yang dinyatakan 'sukses', dan 47 kali *login* pada *password* yang dinyatakan 'sukses'.

User 4 memasukkan kata 'febrianto' sebagai *username* dan *password*. Dari 50 kali *login*, diperoleh 18 kali *login* yang dinyatakan 'sukses', 19 kali *login* pada *username* yang dinyatakan 'sukses', dan 49 kali *login* pada *password* yang dinyatakan 'sukses'.

User 5 memasukkan kata 'julianto' sebagai *username* dan *password*. Dari 50 kali *login*, diperoleh 47 kali *login* yang dinyatakan 'sukses', 49 kali *login* pada username yang dinyatakan 'sukses', dan 48 kali *login* pada *password* yang dinyatakan 'sukses'.

User 6 memasukkan kata 'visualbasic' sebagai *username* dan *password*. Hasil 50 kali *login* diperoleh 50 kali *login* yang dinyatakan 'sukses', 50 kali *login* pada *username* yang dinyatakan 'sukses', dan 50 kali *login* pada *password* yang dinyatakan 'sukses'.

User 7 memasukkan kata 'mahasiswa' sebagai *username* dan *password*. Dari 50 kali *login* yang dilakukan, diperoleh 49 kali *login* yang dinyatakan 'sukses', 50 kali *login* pada *username* yang dinyatakan 'sukses', dan 49 kali *login* pada *password* yang dinyatakan 'sukses'.

User 8 memasukkan kata 'verifikasi' sebagai *username* dan *password*. Dari 50 kali *login*, diperoleh 46 kali *login* yang dinyatakan 'sukses', 49 kali *login* pada *username* yang dinyatakan 'sukses', dan 47 kali *login* pada *password* yang dinyatakan 'sukses'.

User 9 memasukkan kata 'tunjangan' sebagai *username* dan *password*. Dari 50 kali *login*, diperoleh 39 kali *login* yang dinyatakan 'sukses', 43 kali *login* pada *username* yang dinyatakan 'sukses', dan 45 kali *login* pada *password* yang dinyatakan 'sukses'.

Pertukaran Sampel Pengetikan Antar User

***User* 1 Bertindak Sebagai *User* 2**

User 1 akan melakukan *login* sebagai *user* 2 dengan mengetikan *username* dan *password* dari *user* 2. Dari 31 kali *login* yang dilakukan, tidak ada satupun *login* yang berhasil. Berikut adalah hasil *login* user 1:

Tabel 2. Hasil *login user* 1 sebagai *user* 2

Login ke-	*Username*			*Password*			*Login*
	Kecocokan (%)	Bobot (%)_	*Login*	Kecocokan (%)	Bobot (%)_	*Login*	
1	93.33	95.75	Sukses	100	100	Sukses	Sukses
2	73.33	69.91	Gagal	100	100	Sukses	Gagal
3	86.67	79.94	Gagal	100	100	Sukses	Gagal
4	93.33	92.41	Sukses	100	100	Sukses	Sukses
5	93.33	96.95	Sukses	100	100	Sukses	Sukses
6	100	100	Sukses	100	100	Sukses	Sukses
7	86.67	89.82	Sukses	66.67	69.17	Gagal	Gagal
8	100	100	Sukses	86.67	83.50	Sukses	Sukses

9	80	82.06	Sukses	100	100	Sukses	Sukses
10	100	100	Sukses	100	100	Sukses	Sukses

***User* 1 Bertindak Sebagai *User* 3**

User 1 akan melakukan *login* sebagai *user* 3 dengan mengetikan *username* dan *password* dari *user* 3. Dari 31 kali *login* yang dilakukan oleh *user* 1, tidak ada satupun *login* yang berhasil.

Tabel 3. Hasil *login user* 1 sebagai *user* 3

Login ke-	*Username*			*Password*			*Login*
	Kecocokan (%)	Bobot (%)_	*Login*	Kecocokan (%)	Bobot (%)_	*Login*	
1	93.33	95.75	Sukses	100	100	Sukses	Sukses
2	73.33	69.91	Gagal	100	100	Sukses	Gagal
3	86.67	79.94	Gagal	100	100	Sukses	Gagal
4	93.33	92.41	Sukses	100	100	Sukses	Sukses
5	93.33	96.95	Sukses	100	100	Sukses	Sukses
6	100	100	Sukses	100	100	Sukses	Sukses
7	86.67	89.82	Sukses	66.67	69.17	Gagal	Gagal
8	100	100	Sukses	86.67	83.50	Sukses	Sukses
9	80	82.06	Sukses	100	100	Sukses	Sukses
10	100	100	Sukses	100	100	Sukses	Sukses

Analisis Hasil Pengujian Oleh User

Tabel 4. Analisis hasil pengujian

User	Jumlah Login	Login Sukses (%)	Login Username Sukses (%)	Login Password Sukses (%)
1	50	92	96	96
2	50	48	60	78
3	50	92	96	94
4	50	36	38	98
5	50	94	98	96
6	50	100	100	100
7	50	98	100	98
8	50	92	98	94
9	50	78	86	90
Rata-Rata		81.11	85.78	93.78

Dari tabel 4 di atas, diperoleh rata-rata login yang berhasil adalah 81.11%. Ini berarti *FRR (False Rejected Rate)* adalah 18.89%.

Analisis Hasil Pertukaran Sampel Pengetikan

Dari tabel 5 tidak terdapat satupun *login* yang berhasil masuk ketika terjadi pertukaran sampel pengetikan. Ini berarti *FAR (False Acceptance Rate)* sebesar 0%.

Tabel 5. Analisis hasil pertukaran sampel pengetikan

User	Jumlah *Login*	*Login* Sukses (%)	*Login Username* Sukses (%)	*Login Password* Sukses (%)
User 1 bertindak sebagai *User* 2	31	0	0	0
User 1 bertindak sebagai *User* 3	31	0	0	100
Rata-rata		0	0	50

5. Kesimpulan

Berdasarkan pada pembahasan-pembahasan sebelumnya, hasil-hasil implementasi, dan analisis terhadap sampel pengetikan dengan metode yang telah dibahas, maka didapatlah beberapa kesimpulan yaitu:Hasil *FRR* yakni 18.89% menunjukkan hasil yang mengecewakan, mengingat dari literatur yang diperoleh, hasil *FRR* di bawah 10%. Tetapi hasil *FAR* yakni 0% menunjukkan bahwa sistem sulit untuk ditembus. Hasil *FRR* yang tidak begitu bagus tidak berarti perangkat lunak ini tidak berjalan dengan semestinya, tetapi hasil tersebut lebih dipengaruhi dari jumlah user yang ikut berpartisipasi dalam penelitian ini serta jumlah login dari masing-masing user.

Dibutuhkan pengetikan yang konsisten sehingga dapat diperoleh sampel pengetikan yang benar-benar dapat mewakili hasil *FAR* dan *FRR*. Untuk mengembangkan perangkat lunak ini agar menjadi lebih efektif dalam melakukan verifikasi terhadap irama pengetikan maka diberikan saran sebagai berikut: Percobaan perlu dilakukan dengan sampel yang banyak agar diperoleh hasil yang efektif. Penambahan faktor-faktor lain yang berpengaruh terhadap irama pengetikan seperti penggunaan jenis *keyboard* yang berbeda, berapa kali *login* dalam satu hari.

6. References

[1] D. Umphress & G. Williams, "Identity Verification Through Keyboard Characteristics", *International Journal of Man-Machine Studies*, vol. 23, no. 3, pp. 263 – 273, 1985.

[2] J. Leggett & G. Williams, "Verifying Identity Via Keystroke Characteristics", *International Journal of Man-Machine Studies*, vol. 28, no. 1, pp. 67 – 76, 1988.

[1] [3] D. Avison & G. Fitgerald, *Information System Development: Methodologies, Techniques, and Tools*, 4th ed. United Kingdom: McGrow Hill, 2006.