BAB I
PENDAHULUAN

1.1 Latar Belakang

Informasi adalah hal penting baik untuk individu maupun suatu instansi. Saat sebuah informasi hilang, berubah, atau tidak dapat digunakan akan berakibat pada timbulnya kerugian baik secara material maupun non-material (Tiwari, 2012). Menurut Shirkant Tiwari tahun 2012 mengatakan bahwa *hacker* atau pihak yang tidak seharusnya mengakses suatu informasi telah merugikan dengan cara mengakses informasi tersebut menggunakan akun yang sah.

Untuk mengakses suatu informasi yang sah, seorang *user* harus melewati tiga proses antara lain *Authentication, Authorization*, dan *Accounting* (Todorov, 2007). Dimulai dari proses *authentication* yang terbagi menjadi *identification* dan *actual authentication* (Todorov, 2007). Menurut Dobromir Todorov, *identification* adalah proses memasukkan identitas *user* ke dalam sistem kemudian sistem akan mencari pada identitas yang dimasukkan terdapat pada sistem. Identitas yang dimaksud dapat berupa *user id* dan *password* serta PIN, sedangkan *actual authentication* merupakan proses untuk memvalidasi identitas yang dimasukkan oleh *user*.

Password dan PIN adalah salah satu identitas yang digunakan pada proses autentikasi dengan memasukkan *Something We Know* (Tiwari, 2012). Segala sesuatu yang harus diingat untuk membuktikan seseorang berhak atas informasi yang akan diakses adalah metode autentikasi *Something We Know* (Tiwari, 2012). Menurut Shrikant Tiwari pada penelitian yang berjudul Internet Security Using Biometrics tahun 2012 mengatakan bahwa penggunaan segala sesuatu yang

berhubungan dengan metode *Something We Know* memiliki kelemahan seperti dapat dicuri, dapat dibagikan, dan mudah ditebak. Selain metode tersebut, terdapat metode *Something We Are* yang lebih dikenal sebagai *Biometric* (Tawari, 2012).

Menurut Aleksandra Babich pada tesisnya tahun 2012, *biometric* terbagi atas 2 tipe, yaitu *physiological* dan *behavior*. *Behavior* memungkinkan seseorang atau individu mengautentikasikan dirinya dengan menggunakan perilaku atau kebiasaan yang dimilikinya salah satunya adalah ritme pengetikan menggunakan *keyboard*, sedangkan *physiological* dalam melakukan proses autentikasi memerlukan ciri khusus yang terdapat pada anggota tubuh.

Penggunaan komputer yang tidak hanya untuk bekerja melainkan juga untuk hiburan, komunikasi dan pendidikan menjadikan mengetik menggunakan *keyboard* adalah bagian pada kehidupan sehari-hari (Babich, 2012). Orang-orang menggunakan *keyboard* dengan keunikannya masing-masing, beberapa orang mengetik dengan cepat dan beberapa orang mengetik dengan lambat. Hal tersebut menjadikan *keystroke recognition* sebagai cara natural untuk mengautentikasi seseorang dalam mengakses suatu informasi (Babich, 2012). Hal tersebut dimungkinkan dengan melihat pola mengetik dari seseorang menggunakan *keyboard* atau dapat juga disebut *keystroke*. Dalam *biometric keystroke recognition* yang terpenting adalah bagaimana hal tersebut diketik bukan pada apa yang diketik (Babich, 2012). Beberapa keuntungan menggunakan *keystroke* adalah tidak diperlukannya *hardware* tambahan dan proses pengambilan datanya tidak terlalu mengubah perilaku proses autentikasi pada umumnya. Hingga tahun 2016, terdapat sistem autentikasi menggunakan keystroke berbentuk sistem application programming interface (API) yang dibangun oleh perusahaan bernama TM3

Software GmbH. Namun, sistem tersebut bersifat komersial sehingga sistem yang dibangun tersebut bersifat tertutup.

Menurut Magalhaes, dkk. tahun 2009 pada penelitian yang berjudul Keystroke Dynamics and Graphical Authentication Systems mengatakan bahwa terdapat dua pendekatan yang dapat dilakukan untuk menganalisa *keystroke*, yaitu dengan *machine learning* atau algoritma deterministik. Hingga pada 2012 pada penelitian yang berjudul Biometric Authentication and Identification using Keystroke Dynamic: A Survey, Salil P. Banerjee mengatakan terdapat pendekatan yang dapat digunakan untuk menganalisis *keystroke*, yaitu *Statistical Algorithm*, *Neural Network, Pattern Recognition*, dan analisa *heuristic*. Penggunaan *neural network* pada penelitian *keystroke dynamic* menunjukkan hasil yang cukup baik (Banerjee, 2012). Hal tersebut dikarenakan *neural network* yang dapat menangani beberapa parameter dalam menganalisis *keystroke dynamic* (Banerjee, 2012). Meskipun memiliki kekurangan berupa waktu *training* yang dapat berlangsung lama, tetapi menurut Salil P. Benerjee pada tahun 2012, penggunaan *machine learning* untuk menganalisis *keystroke* dapat diandalkan.

Pada tahun 2008, Rifki Fabianto dalam skripsi yang berjudul Penerapan Dinamika Keystroke untuk Otentikasi Sistem Keamanan *Login* Aplikasi dengan *Metode Fuzzy Logic* telah berhasil mengimplementasikan metode *keystroke dynamic*. Dalam penelitian tersebut, parameter yang digunakan sebagai alat ukur *keystroke dynamic* adalah waktu rata-rata tekan pada *tuts keyboard* dan waktu tunggu.

Pada tahun 2010, Nurul Hasanah mengembangkan skripsi yang dibuat oleh Rifki Fabianto dengan menggunakan metode *Neo Fuzzy Neuron*. Dengan tingkat

reliabilitas hingga 80%, sistem tersebut dapat melakukan validasi *login* dengan parameter waktu rata-rata tekan pada *tuts keyboard* dan waktu rata-rata verifikasi *login.*

Pada tahun 2003, sebuah penelitian yang dibuat oleh Venu G. Gudise dan K. Venayagamoorthy menunjukkan bahwa *Particle Swarm Optimization* (PSO) dapat digunakan sebagai salah satu alternatif algoritma dalam proses *training neural network* untuk mencari bobot yang optimal pada jaringan saraf tiruan. Penelitian tersebut menunjukkan performa PSO yang lebih baik dibandingkan *Backpropagation* dalam aplikasi yang membutuhkan *training* yang cepat dalam *neural network.*

Berdasarkan pemaparan di atas, maka akan diimplementasikan *keystroke dynamic* sebagai alat autentikasi *user* menggunakan jaringan saraf tiruan dengan algoritma *particle swarm optimization* sebagai algoritma pada proses *training* jaringan saraf tiruan.

1.2 Rumusan Masalah

Bagaimana mengimplementasikan *keystroke dynamic* sebagai alat dalam melakukan autentikasi *user* dengan menggunakan jaringan saraf tiruan dan algoritma *particle swarm optimization* dalam proses *training* jaringan saraf tiruan?

1.3 Batasan Masalah

Beberapa batasan pada penelitian kali ini adalah sebagai berikut.

1. Dari lima parameter *keystroke dynamic*, penelitian ini hanya menggunakan empat, yaitu *flight time, dwell time, overall speed*, dan *error rate.*

2. *Keyboard* yang digunakan adalah *keyboard* dengan susunan QWERTY.
3. Selama proses pengambilan data dan uji coba kepada *user*, akan digunakan *keyboard* dengan jenis yang sama.
4. Kalimat yang digunakan untuk proses *training* adalah kalimat berbahasa Indonesia.
5. Proses pengambilan data dan *traning* data akan dilakukan terpisah.
6. Jumlah kalimat dalam setiap data pada proses *training* berkisar dari 1-3 kalimat.
7. Sistem *training* akan menggunakan bahasa pemrograman C# menggunakan data yang berada pada *database*.
8. Sistem autentikasi dan pengambilan data akan menggunakan bahasa pemrograman PHP dan javascript.
9. Jumlah data pada proses pelatihan berjumlah 15 data per user.

1.4 Tujuan penelitian

Penelitian kali ini bertujuan untuk mengimplementasikan *keystroke dynamic* sebagai alat dalam melakukan autentikasi *user* dengan menggunakan jaringan saraf tiruan dan algoritma *particle swarm optimization* dalam proses *training* jaringan saraf tiruan.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitan ini adalah membantu pihak pengembang *website* ataupun sistem lainnya menyediakan proses autentikasi selain mengetikkan *password* seperti biasanya. Penerapan *keystroke dynamic* ini juga

diharapkan dapat mengurangi penyalahgunaan sistem meskipun *password*-nya sudah diketahui.

1.6 Sistematika Penulisan

Sistematika penulisan dalam penelitian ini terdiri dari lima bab, yaitu sebagai berikut.

1. BAB I PENDAHULUAN

   Bab ini menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan manfaat penelitian, serta sistematika penulisan tentang penjelasan singkat dari setiap bab.

2. BAB II LANDASAN TEORI

   Bab ini berisi landasan-landasan teori yang melandasi penelitian ini, seperti *biometric*, *keystroke dynamic*, jaringan saraf tiruan, dan *particle swarm optimization*.

3. BAB III METODOLOGI DAN PERANCANGAN SISTEM

   Bab ini berisi tentang metode penelitian yang digunakan, perancangan aplikasi, seperti rancangan arsitektur jaringan saraf tiruan, *data flow diagram*, *sitemap*, *flowchart*, *entity relationship diagram*, struktur tabel, dan perancangan desain antarmuka.

4. BAB IV IMPLEMENTASI DAN UJI COBA

   Bab ini berisi tentang spesifikasi sistem yang digunakan untuk menjalankan aplikasi, implementasi aplikasi yang dibangun, dan uji coba aplikasi yang dibangun.

5. BAB V SIMPULAN DAN SARAN

Bab ini berisikan simpulan yang didapat sesuai dengan hasil pengujian aplikasi dan saran mengenai pengembangan aplikasi selanjutnya.