SISTEM PENGAMANAN PENGINPUTAN NILAI DOSEN PADA SISTEM INFORMASI AKADEMIK BERBASIS SMS

Asnurul Isroqmi
Universitas PGRI Palembang
e-mail: asnurul@gmail.com

Abstrak— Sistem informasi akademik di universitas sangat penting untuk kegiatan akademik dosen dan mahasiswa yang begitu dinamis, tetapi ini tidak ada artinya jika tidak didukung oleh tingkat keamanan yang baik dari sistem itu sendiri, terutama bagi dosen yang tidak terbiasa dengan penguasaan Teknologi Informasi . Salah satu hal penting dalam sistem informasi akademik adalah ketika memasukkan nilai siswa pada akhir semester, perlu memiliki sistem keamanan yang dapat dikontrol oleh dosen itu sendiri walaupun dosen tersebut tidak benar-benar mengendalikan teknologi informasi. Inovasi dalam membuat fitur One Time Password (OTP) yang dikirimkan ke telepon seluler dosen pengguna melalui Layanan Pesan Singkat (SMS) ketika nilai dikumpulkan, adalah sistem keamanan yang sederhana namun dapat diandalkan. Penelitian ini bertujuan untuk membahas aplikasi keamanan untuk mengakses Sistem Informasi Akademik berbasis WEB ketika dosen membuat skor input, dalam bentuk keamanan menggunakan One Time Password yang dihasilkan dari program acak dan hash MD5 yang menghasilkan kode SMS untuk otentikasi.

Kata Kunci— Sistem Informasi Akademik; Input Nilai Dosen; One Time Password; Hash MD5.

Abstract— *Academic information systems in universities are very important for academic activities of lecturers and students who are so dynamic, but this is meaningless if it is not supported by a good level of security of the system itself, especially for lecturers who are unfamiliar with mastering Information Technology. One of the important things in academic information systems is when inputting student grades at the end of the semester, it is necessary to have a security system that can be controlled by the lecturer himself even though the lecturer does not really control information technology. The innovation in making the One Time Password (OTP) feature that is sent to the user's lecturer cellular phone through Short Message Service (SMS) when value is collected, is a simple but reliable security system. This study aims to discuss the application of security to access the WEB-based Academic Information System when lecturers make inputting scores, in the form of security using One Time Password generated from random programs and MD5 hashes that generate an SMS code for authentication.*

Keywords— *Academic Information Systems; Lecturer Value Input; One Time Password; Hash MD5*.

PENDAHULUAN

Pada saat ini dunia telah memasuki era revolusi industri 4.0 atau revolusi industri dunia keempat, dimana teknologi informasi menjadi basis kehidupan manusia hampir di semua aktivitas, tidak terkecuali di perguruan tinggi. Sistem informasi akademik di perguruan tinggi merupakan suatu kebutuhan yang sudah selayaknya untuk dipenuhi. Menurut Satoto (2009) Sistem Informasi Akademik adalah perangkat lunak yang digunakan untuk menyajikan informasi dan menata administrasi yang berhubungan dengan kegiatan akademis.

Kebutuhan sistem informasi akademik di perguruan tinggi dilandasi oleh kegiatan akademik baik oleh mahasiswa maupun

dosen yang begitu dinamis. Penyajian informasi tidak hanya perlu ditata dengan baik namun juga dapat diakses dengan cepat di setiap saat dari berbagai tempat, sehingga memudahkan dosen dan mahasiswa memberikan atau menerima informasi berkenaan dengan kegiatan akademik. Untuk menjawab kebutuhan ini dibeberapa perguruan tinggi saat ini telah menggunakan perangkat lunak atau aplikasi sistem informasi akademik yang berbasis web.

Salah satu kelebihan aplikasi berbasis web adalah dapat diakses dimana saja selama pengguna dapat terhubung dengan internet tanpa perlu membawa atau menginstal file program terlebih dahulu. Namun kelebihan ini tidak ada artinya, jika aplikasi dari sistem informasi ini tidak didukung dengan sistem keamanan yang baik. Keamanan merupakan salah satu aspek yang sangat penting untuk diperhatikan, karena dengan banyaknya user atau pengguna komputer yang terhubung dalam suatu jaringan maka data ataupun informasi menjadi hal yang sangat rentan terhadap serangan-serangan yang tidak diinginkan. Beberapa cara bisa diterapkan oleh *hacker* untuk mengetahui username dan password dari pengguna, salah satunya adalah dengan *sniffing* atau yang sering dikenal dengan istilah password sniffing, yaitu teknik pencurian password menggunakan bantuan perangkat lunak dengan mengambil informasi remote login seperti username dan password (Wang, 2009).

Berdasarkan banyak penelitian-penelitian yang telah dilakukan sebelumnya tentang keamanan sistem *login,* semuanya memberikan pemahaman bahwa sistem *login* sangat penting dalam mengakses aplikasi sistem informasi berbasis web. Dua penelitian berikut memberikan gambaran bagaimana keamanan dalam sistem login.

Penelitian (1) "*Ananlisis Keamanan Sistem Login* " oleh Dyana Marisa Khairina tahun 2011. Penting sekali memperhatikan pengamanan pada saat login, dengan mengenkripsi pada password sebelum dikirimkan server. Kombinasi enskripsi MD5 dan program pengacak dapat menjaga keamanan atau integritas data lebih baik, dibandingkan hanya mengenkripsi dengan MD5. (Khairina, 2011)

Penelitain (2) "*Studi Pengamanan Login Pada Sistem Informasi Akademik Menggunakan Otentifikasi One Time Password Berbasisis SMS dengan Hash"* oleh Kartika Imam Santoso dkk. tahun 2013. Dengan memberlakukan pemberian OTP (*one time password*) pada saat login, dan OTP dienkripsi dengan hash MD5 sehingga sulit ditebak oleh hacker, menjadikan sistem pengamanan login yang jauh lebih baik (Santoso, 2013).

Terhadap sistem informasi akademik yang kurang memperhatikan keamanan sistem login, maka pencurian password semakin mudah dilakukan oleh *hacker* jika pengguna sistem informasi tidak begitu memahami teknologi informasi. Sebagian dosen pengguna aplikasi sistem informasi masih sangat awam terhadap keamanan sistem informasi. Beberapa dosen seringkali menggunakan password yang

mudah ditebak, bahkan password dibuat sama persis dengan *user name* yang digunakan.

Permasalahan berikutnya adalah seringkali pada saat penginputan data, misalnya menginput nilai mahasiswa diserahkan kepada pihak lain. Penyerahan peng-inputan kepada pihak lain bisa jadi disebabkan oleh karena dosen masih terlalu awam terhadap teknologi informasi atau dosen terlalu sibuk dengan kegiatan lain.

Untuk beberapa pemggunaan fitur pada aplikasi sistem informasi akademik oleh dosen yang sifatnya tidak menginput atau melakukan perubahan data, dengan kata lain hanya membaca data atau informasi, misalnya melihat jadwal perkuliahan, maka keamanan tidak begitu menjadi hal yang penting. Namun menjadi berbeda bila seorang dosen harus melakukan penginputan data atau perubahan data misalnya meng-input nilai mahasiswa, maka perlu melakukan inovasi sistem keamanan. Otentikasi ulang, untuk meyakinkan apakah yang melakukan penginputan nilai adalah benar-benar dosen yang bersangkutan mutlak diperlukan, atau paling tidak dosen yang bersangkutan memiliki perangkat sebagai alat kontrol pemberi izin sebelum melakukan penginputan nilai.

Dari permasalan diatas maka fokus kajian dari tulisan ini adalah untuk membahas sistem pengamanan yang dapat digunakan ketika dosen harus meng-input nilai mahasiswa kedalam sistem informasi akademik, walaupun dosen masih sangat awam terhadap kemajuan teknologi informasi itu sendiri. Bahkan sekalipun dosen harus menyerahkan penginputan nilai kepada pihak lain, namun ia tetap memiliki kontrol sebagai pemilik akun dari sistem informasi akademik melalui Otentikasi One Time Password (OTP) berbasis SMS yang dienkripsi dengan MD5.

PEMBAHASAN

A. Perangkat Sistem Informasi

Beberapa hal yang sering kali ditemui berkenaan dengan aplikasi atau perangkat lunak, terutama sekali yang berkaitan dengan sistem informasi berbasis web.

a. Keamaan Login Sistem Informasi.

1. Authentication

Authentifaction atau otentikasi bertujuan untuk membuktikan siapa pengguna sebenarnya, apakah yang sedang menggunakan aplikasi benar-benar orang yang diklaim sebagai pemilik akun yang sedang digunakan.

Terdapat 3 kategori metode untuk otentifikasi, yang semunya berhubungan dengan pengguna itu sendiri;

- *Something You Know*

  Metode otentikasi yang paling umum. Cara ini mengandalkan kerahasiaan informasi, misalnya usernamae, password dan PIN, diasumsikan bahwa tidak ada seorangpun yang mengetahui rahasia itu kecuali pengguna aplikasi itu sendiri.
- *Something You Have*

  Menggunakan faktor tambahan untuk membuat otentikasi menjadi lebih aman, dengan mengandalkan barang

yang dimiliki oleh pengguna tersebut yang sifatnya unik misalnya kartu magnetik/smartcard, hardware token, dan lain sebagainya, Diasumsikan bahwa tidak ada seorangpun yang memiliki barang tersebut kecuali pengguna itu sendiri.

- *Something You Are*
  Metode ini mengandalkan keunikan bagian-bagian tubuh, sidik jari, suara atau sidik retina. Diasumsikan bahwa bagian tubuh seseoang tidak mungkin sama dengan orang lain.

2. *Two Factor Authentication*

Pada aplikasi tertentu yang lebih kritis dan sensitif misalnya transaksi keuangan, maka satu metode otentikasi tidak cukup, perlu menggunakan dua faktor (metode) yang berbeda. Contohnya saat menggunakan kartu ATM. Mengakses rekening tabungan melalui mesin ATM memerlukan dua faktor keamanan yang berbeda yaitu kartu ATM itu sendiri disebut sebagai “something you have” dan PIN yang disebut sebagai “something you know”

3. *Password Token*

Aplikasi internet banking umumnya dilengkapi dengan sebuah alat untuk menghasilkan password token. Nasabah bank diberikan alat ini untuk dapat mengakses layanan bank. Setiap kali transaksi, nasabah harus menginputkan kode token yang dikeluarkan oleh alat ini ke web perbankan.

Pada umumnya ada dua mode pemakaian token internet banking:

- *Mode Challenge/Response (C/R).*
  Mode ini merupakan mode yang paling seringkali digunakan untuk bertransaksi. Cara kerja dalam mode ini yaitu, web server mengeluarkan kode satu deretan angka. Angka ini kemudian dimasukkan kedalam mesin token oleh pengguna untuk memperoleh respon atau kode berikutnya atau yang disebut dengan token. Kode dari alat token selanjutnya dimasukkan ke dalam form di situs internet banking. Token akan mengeluarkan kode yang berbeda-beda walaupun dengan challenge kode yang sama secara periodik tergantung waktu ketika challenge dimasukkan ke dalam token.
- *Mode Self Generated (Response Only)*
  Berbeda dengan sebelumnya, dalam mode ini token pengguna dapat langsung mengeluarkan sederetan angka tanpa harus memasukkan kode *challenge* dari web. Seperti halnya mode C/R, token juga mengeluarkan kode yang berbeda-beda secara periodik tergantung waktu ketika token diminta untuk menghasilkan kode self generated.

Kode yang dikeluarkan oleh token baik dalam mode C/R maupun Self Generated (resopnse only) tidak lain adalah bentuk password juga. Perbedaannya adalah password dipakai untuk login, memiliki keterbatasan untuk alasan keamanan, yaitu: hanya boleh dipakai 1 kali, atau yang sering kali disebut dengan OTP (*One Time Password*).

b. One Time Password

One Time Pssword adalah sebuah *password* yang hanya berlaku untuk sesi login tunggal atau transaksi tunggal (Wang, 2009).

Algoritma dari OTP dapat dibuat secara *random*. Terdapat tiga pendekatan utama dalam proses *generate* OTP yaitu; (1) berdasarkan "*time-synchronization*" antara otentikasi *server-client* yang menyediakan *password* (OTP akan bersifat valid bila dalam peride waktu yang singkat), (2) berdasarkan "*mathematical algorithm*" yang memungkinkan generalisasi suatu *password* baru berdasarkan *password* sebelumnya, (3) berdasarkan "*mathematical algorithm*", *password* baru didasari oleh suatu tantangan (misalnya : penetapan nilai suatu *password* secara *random* akan ditentukan oleh server atau detail transaksinya) (Wang, 2009).

Program pembuatan one time password ini ditanamkan dalan aplikasi sistem informasi akademik. Saat dosen melakukan klik tombol penginputan nilai maka program secara otomatis menghasilkan token. Token dibuat dibuat acak dan selalu berubah, dimana yang menjadi input untuk memproduksi token ini dapat melibatkan data base dari nama atau kode dosen itu sendiri, nomor telepon seluler, tanggal dan waktu. Input dari tanggal dan waktu inilah sebagai variabel sehingga dapat membuat token yang tidak pernah sama dalam setiap waktu.

Token, one time password, merupakan sistem keamanan yang sangat handal, karena ia hanya berlaku 1 kali dan masa berlakunya juga dapat dibatasi, diatur sedemikian rupa misalnya 1 menit, 30 menit, 1 jam, 1 hari dan seterusnya. Sistem keamanan seperti ini juga dapat diterapkan kedalam layanan sistem informasi akademik terutama untuk hal-hal yang sifatnya kritis, misalnya penginputan nilai mahasiswa oleh dosen.

c. Alat Komunikasi Telepon seluler

Di era sekarang ini hampir semua orang memiliki telepon seluler. Fungsi telepon seluler tidak hanya sebatas sebagai alat komunikasi. Pemilik akun dari suatu sistem informasi biasanya diminta untuk memasukkan nomon telepon seluler sebagai identitas diri dari pemilik akun itu sendiri. Dan tidak sedikit pula di beberapa layanan sistem informasi yang ada menjadikan nomor telepon seluler sebagai password untuk dapat masuk kedalam sistem.

Dengan memanfaatkan jaringan internet saat ini, maka telepon seluler juga dapat digunakan sebagai alat komunikasi, bukan komunikasi dalam pengertian melakukan pembicaraan, namun alat komunikasi penyampai pesan teks password, yang dikirimkan dari satu server.

d. Kriptografi MD5

Kriptografi adalah suatu bidang ilmu yang mempelajari cara agar data atau pesan saat dikirimkan dari pihak pengirim ke pihak penerima tetap terjaga dengan aman tanpa ada gangguan dari pihak ketiga (Stalling, 2005).

MD5 singkatan dari Message Digest 5 yang merupakan fungsi hash kriptografi.

MD5 ini ditemukan oleh Ronald Rivest pada tahun 1991, idenya adalah mengambil data acak baik tulisan atau biner sebagai input dan menghasilkan ukuran nilan hash tetap sebagai outputnya. Outpunya inilah yang menjadi pesan baru yang dimanfaatkan menjadi kode atau password baru, sehingga dapat meningkatkan keamanan dari suatu file, akun atau tulisan dari pencuri password, *hacker.* Hal ini dapat terjadi dikarenakan apa yang dibaca baca oleh *hacker* adalah kumpulan digit hex bukan string asli tulisan itu sendiri yang dibuat sebelumnya.

B. Token Telepon seluler

Perkembangan teknologi informasi dan komunikasi telah memungkinkan terjadinya koneksi antara telepon seluler dan unit komputer. Keduanya dapat berkomunikasi melalui jaringan internet dimana keduanya dapat berkomunikasi dengan server, sehingga dapat melakukan proses otentikasi sebelum dapat mengakses sistem informasi. Respon terhadap Permintaan otentikasi dari web suatu sistem informasi dapat di respon melalui pengiriman SMS lewat telepon seluler, sehingga pengguna selanjutnya dapat menyelesaikan proses otentikasi dengan menanggapi SMS yang diterima dengan mengirimkan pesan singkat melalui Web (Stalling, 2005).

Melalui jaringan internet, maka dapat dibangun komunikasi antar komputer server milik suatu badan/lembaga dengan badan/lembaga lainnya. Dengan koneksi antar jaringan ini maka dapat dimanfaatkan untuk mengirimkan pesan atau teks password dari server sistem informasi akademik ke server penyedia layanan telepon seluler untuk diteruskan ke pemilik nomor telepon seluler melalui pesan singkat, SMS.

Dari pembahasan sebelumnya diatas berkenaan dengan perangkat sistem informasi, maka dengan menggunakan perangkat yang ada yang sudah tersedia, dapat dibuat suatu bentuk inovasi untuk menghasilkan kode/password berupa token untuk dapat membuka atau mengakses aplikasi sistem informasi. Kode token dapat dihasilkan untuk disampaikan kepada pengguna atau pemilik akun dari sistem informasi tanpa harus menggunakan alat token seperti yang disediakan oleh perbankan, cukup dengan memanfaatkan telepon seluler, apalagi di era saat ini hampir semua orang sudah memilikinya.

C. Otentifikasi Penginputan Nilai

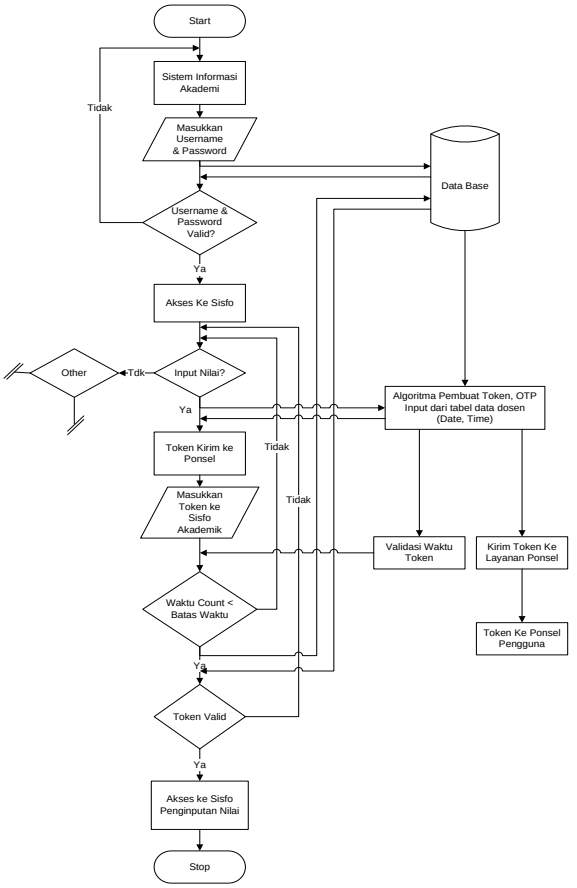
Otentifikasi dilakukan diawal untuk membuka atau mengakses aplikasi sistem informasi, dan umumnya tidak menggunakan kode token cukup hanya menginput user name dan password. Kode token digunakan hanya ketika pengguna harus mengakses hal-hal yang kritis, misalnya untuk menginput data atau merubah data.

Pada sistem informasi akademik salah satu hal yang kritis adalah ketika dosen harus menginput nilai-nilai mahasiswa setelah menyelesaikan ujian akhir semester. Guna meningkatkan keamanan maka perlu dilakukan otentifikasi ulang untuk mengkonfirmasi apakah dosen yang akan

menginput nilai adalah benar-benar dosen bersangkutan.

Otentifikasi ulang dapat dilakukan dengan penerapan pengisian kode token. Saat dosen mengakses tombol layar pengisian nilai, maka sistem pada server secara otomatis akan membuat kode token yang dikriptografi dengan MD5. Kode token dibuat acak dan selalu berubah setiap waktu. Kemudian melalui jaringan internet hasilnya dikirimkan ke server penyedia layanan telepon seluler untuk diteruskan ke telepon seluler milik dosen yang bersangkutan.

Alur data atau informasi sistem aplikasi keamanan saat penginputan nilai dengan memberlakukan layanan OTP berbasis SMS dapat dilihat pada gambar berikut;



Gambar. Alur Sistem Keamanan Dengan One Time Password (OTP)

Penerapan pengisian kode token ini dilakukan setiap kali dosen menginput nilai dari satu mata kuliah, dan kode token diberikan batas waktu berlaku. Melalui sistem pengamanan seperti ini maka dosen yang masih sangat awak dengan teknologi informasi, bahkan sekalipun harus menyerahkan penginputan nilai kepada orang lain, maka kontrol tetap ada pada dosen yang bersangkutan.

Dan guna meningkatkan sistem keamanan agar terhindar dari pencurian password oleh *hacker*, maka kode token yang sifatnya one time password, terlebih dahulu di enkrip melalui kriptografi MD5 sebelum kode tersebut dikirimkan ke penyedia lanyanan telepon seluler, untuk disampaikan ke telepon seluler dosen yang bersangkutan.

Dengan demikian pemberlakuan layanan token one time password (OTP) tidak dilakukan setiap kali dosen harus login untuk membuka dan mengakses sistem informasi akademi. Token OTP diberlakukan hanya ketika dosen harus menginput nilai mahasiswa, karena frekuensi penginputan nilai tidak terlalu sering dilakukan, hanya dilakukan di akhir semester. Disamping tidak membuat dosen kuwalahan saat harus login ke sistem informasi akademik juga dapat menghemat biaya pengeluaran untuk SMS.

Pemberlakuan layanan ini tidak hanya dapat diterapakan untuk penginputan nilai, namun juga untuk tindakan lainnya misalnya dosen lupa password untuk masuk ke dalam ke sistem informasi. Reset password atau membuat password baru dapat dapat dilakukan dengan layanan token juga.

KESIMPULAN

Sistem informasi akademik berbasis web merupakan sistem inforamsi yang handal untuk diterapkan mengingat aktivitas dosen dan mahasiswa yang begitu dinamis, namun perlu peningkatan sistem keamanan karena sistem sudah masuk dalam jaringan internet. Sistem keamanan dapat ditingkatkan dengan menerapkan pemberian token untuk setiap kali dosen melakukan tindakan kritis pada sistem informasi akademik, misalnya penginputan nilai dosen untuk mahasiswa yang mengikuti mata kuliahnya. Peningkatan keamanan ini perlu dilakukan karena selain sistem sudah masuk kedalam jaringan internet, juga sebagai tindakan antisipasi pengamanan bagi dosen yang masih awam terhadap teknologi informasi ataupun dosen yang sering melakukan penyerahan penginputan nilai kepada pihak lain.

Dengan memberlakukan penginputan token ke dalam form web sistem informasi akademik setiap kali harus melakukan penginputan nilai lewat layanan SMS melalui telepon seluler yang dimiliki oleh dosen yang bersangkutan, maka kontrol terhadap penginputan nilai ataupun tindakan kritas lainnya dapat dijaga oleh dosen.

DAFTAR PUSTAKA

1. Khairina, D. M. (2011). Analisis Keamanan Sistem Login. Jurnal Informatika Mulawarman Vol. 6 No. 2. FMIPA Universitas Mulawarman
2. Santoso, K. I., dan Eko, S. S. (2013). Studi Pengamanan Login Pada Sistem Informasi Akademik Menggunakan Otentifikasi One Time Password Berbasisis SMS dengan Hash MD5. Jurnal Sistem Informasi Bisnis 01.
3. Satoto, K.I. (2008). Analisis keamanan sistem informasi akademik berbasis web di Fakultas Teknik Universitas Diponegoro, Prosiding Seminar Nasional Aplikasi Sains dan Teknologi, Yogyakarta, Desember 13, 175–186
4. Stalling, W. (2005). Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall.
5. Wang, J. (2009). Computer Network Security Theory and Practice, Higher Education Press, Beijing.