**SNASTIKOM 2020**
**Program Studi Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan**
**website: www.snastikom.com**

# SMART LOGIN PADA WEBSITE DENGAN MENGGUNAKAN QR CODE DAN OTENTIKASI ONE TIME PASSWORD

**Lois Adelson**
Universitas Harapan Medan, Jl. H.M. Joni, No. 70 C, Medan, adelsonlois6@gmail.com

**Dodi Siregar**
Universitas Harapan Medan, Jl. H.M. Joni, No. 70 C, Medan,

**Kalvin Chiuloto**
Universitas Harapan Medan, Jl. H.M. Joni, No. 70 C, Medan, kalvin.chiuloto@yahoo.com

**Abstract**

Abstract - The use of passwords has been used in many ways such as logging into a website application. However, most of these passwords still use static passwords, making them vulnerable to tapping login passwords. There are many ways that hackers can do to hack into websites that use a login system, such as phishing techniques. Layered security is required to secure the login system, the use of the OTP code is one way of verification and can only be accessed by the user himself so that it can reduce the potential for wiretapping of access rights. The application of QR Code technology is quite practical and provides an easy solution to enter the system. Users don't need to log in by entering their username and password repeatedly, just pointing the QR Code at the webcam to be scanned. To increase login security to prevent intrusion into the system, authentication is made in the form of a unique, single-use code called One Time Password (OTP). The password that previously used one username and one password will be added to another random password which will be sent to the user's cellular phone via SMS message. This research is able to provide convenience when accessing a QR Code login and increasing security in the system because the OTP code that is sent is only valid for one login session and is valid for only 5 minutes, so the OTP code cannot be reused in the next login session.

**Keywords:**
*Smart Login, Website, QR Code, Authentication, One Time Password*

.

**Abstrak**

Penggunaan password telah digunakan pada banyak hal seperti login ke dalam sebuah aplikasi website.Namun penggunaan password tersebut kebanyakan masih menggunakan password statis sehingga rentan terhadap penyadapan password login. Banyak cara yang bisa dilakukan para hacker untuk melakukan penyadapan pada website yang menggunakan sistem login, seperti teknik phishing. Diperlukan keamanan berlapis untuk mengamankan sistem login tersebut,penggunaan kode OTP merupakan salah satu carauntuk verifikasi dan hanya bisa diakses oleh penggunanya itu sendiri sehingga bisa mengurangi potensi penyadapan hak akses. Penerapan teknologi QR Code ini cukup praktis dan memberikan solusi kemudahan untuk masuk ke dalam sistem.User tidak perlu login dengan memasukkan username dan password berulang kali, cukup mengarahkan QR Code ke webcam untuk dipindai.Untuk meningkatkan keamanan login guna mencegah terjadinya penyusupan kedalam sistem dibuat otentikasi berupa kode unik sekali pakai yang disebut One Time Password (OTP). Password yang sebelumnya menggunakan satu username dan satu password akan ditambah lagi dengan satu random password yang dikirimkan ke telepon selular pengguna lewat pesan SMS. Penelitian ini mampu memberikan kemudahan saat megakses login dengan QR Code serta meningkatkan keamanan pada sistem karena kode OTP yang dikirimkan hanya berlaku untuk satu kali sesi login serta berlaku hanya dalam kurun waktu 5 menit, sehingga kode OTP tidak dapat digunakan kembali pada sesi login berikutnya.

**Kata Kunci:**
*Smart Login, Website, QR Code, Authentication, One Time Password*

## 1. PENDAHULUAN

Salah satu jenis autentikasi yang paling dikenal adalah sistem *login* yang berupa *username* dan *password* yang kemudian dicocokkan ke dalam *database*. Autentikasi berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri [1]. Penggunaan *password* telah digunakan pada banyak hal seperti *login* kedalam sebuah aplikasi *website*. Namun penggunaan *password* tersebut kebanyakan masih menggunakan

*password* statis sehingga apabila didapat oleh pihak yang tidak berwenang maka dapat menimbulkan kerugian. Selain itu proses penginputan *username* dan *password* secara berulang dinilai kurang praktis sehingga perlu dilakukan terobosan dengan cara yang lebih efisien.Kata sandi (*password*) adalah metode otentikasi yang paling sering digunakan di berbagai sistem keamanan. Kemudahan dalam hal implementasi menjadi faktor utama dari pemanfaatan sistem berbasis *password* [2]. Aplikasi *password* manager merupakan salah satu solusiuntuk mengingat *password*, tetapi aplikasi ini memilikiketerbatasan ketika pengguna perlu melakukan autentikasilogin pada perangkat publik [3].

Sehubungan dengan hal tersebut, penggunaan teknologi *QR Code* ini sangat praktis dan menjadi solusi untuk memudahkan masuk ke dalam sistem.*QR Code* merupakan perkembangan dari kode batang atau barcode yang hanya mampu menyimpan informasi secara horizontal sedangkan *QR Code* mampu menyimpan informasi lebih banyak, baik secara horizontal maupun vertikal. *QR Code* dapat menghasilkan 40 versi yang berbeda dari versi 1 (21 x 21 modul) sampai versi 40 (177 x 177 modul).Jika banyak jumlah data yang ditampung, maka diperlukan modul yang banyak juga untuk dan tentu menjadikan QR Code lebih besar lagi [4].Untuk menyampaikan informasi secara cepat dan juga mendapat tanggapan secara cepat adalah merupakan tujuan dari QR Code ini [5].Pada suatu sistem komputer, proses autentikasi biasanya terjadi pada saat masuk (login) atau permintaan akses [6]. Pada penelitian ini user tidak perlu melakukan login dengan memasukkan username dan password secara berulang, cukup mengarahkan *QR Code* ke webcam untuk dipindai serta dengan tambahan penggunaan *One Time Password* (OTP) yang akan diimplementasikan sudah mampu untuk mengatasi masalah tersebut. OTP adalah password yang hanya berlaku untuk satu kali sesi login [7]. OTP menggunakan algoritma pembangkitan dengan sifat semu acak yang telah diuji secara kiptografi [8]. Dalam konteks autentikasi, OTP biasanya digunakan sebagai mekanisme otentikasi tambahan sehingga OTP disebut sebagai dua factor otentikasi (*two-factor-authentication*) [9].

Password yang sebelumnya menggunakan satu *username* dan satu *password* akan ditambahkan dengan satu password acak dikirimkan ke telepon selular pengguna yang akan masuk ke sistem. Password statis yang dimasukkan pada laman login akan diproses pada database dan kemudian server akan men-generate password acak yang kemudian dikirimkan ke telepon selular pengguna. Data dikirimkan berdasarkan nomor telepon selular yang telah didaftarkan pada database.

Penelitian sebelumnyamenerapkan OTP dengan menggunakan algoritma SHA1 dan MD5 untuk meningkatkan keamanan login website, hasil penelitian menunjukan bahwa penerapan OTP dapat mengamankan sistem login website dengan cara memanfaatkan telepon selular android sebagai pengganti token untuk mengimplementasikan OTP [7]. Namun pada aplikasi yang dihasilkan hanya dapat digunakan atau di implementasikan pada smartphone dengan sistem operasi android.Menggunakan telepon selular untuk sarana penerima kode verifikasi sementara agar bisa dimasukkan di halaman verifikasi. Aplikasi ini menggunakan algoritma *Hash* SHA-512 yang berfungsi untuk proses pengkodean yang nantinya hasil dari pengkodean tersebut akan dikirimkan ke telepon selular pengguna yang telah terdaftar di dalam database [10].

Pada penelitian sebelumnya menggunakan OTP untuk proses autentikasi sistem *login* yang dikirimkan ke telepon selular pengguna. Sedangkan pada penelitian ini dengan menambahkan *QR Code* untuk mempermudah proses *login*. Berdasarkan permasalahan yang dikemukakan sebelumnya, perlu dilakukan penelitian untuk mempermudah serta meningkatkan keamanan sewaktu proses *login* ke suatu sistem. Tujuan dari penelitian ini adalah untuk merancang aplikasi sistem keamanan login web menggunakan teknologi *QR Code* dan otentikasi *One Time Password* (OTP), sehingga dapat mempermudah user melakukan login dengan cara yang mudah dan sederhana serta dapat mengamankan sistem autentikasi website sehingga user dapat melakukan login dengan aman tanpa khawatir identitas mereka dicuri.

## 2. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini menghasilkan sebuah aplikasi yang digunakan untuk mempermudah proses *login* ke dalam *website* serta menambahkan keamanan dengan autentikasi. Kata sandi (*password*) adalah metode otentikasi yang paling sering digunakan di berbagai sistem keamanan. Kemudahan dalam hal implementasi menjadi faktor utama dari pemanfaatan sistem berbasis *password* [2].

Aplikasi *password manager* bisa menjadi salah satu solusiuntuk mengingat *password*, tetapi aplikasi ini tentu masih memilikiketerbatasan ketika pengguna perlu melakukan autentikasilogin pada perangkat publik.Pengguna perlu mengetikkan danmengirimkan *password* dari perangkat tersebut ketikamelakukan autentikasi.Hal ini bisa saja beresiko karenaperangkat tersebut rentan terhadap penyadapan data baikmelalui jaringan (man-in-the-middle) maupun perekamanpapan ketik (*key logger*) [3].

Proses *login* konvensional akan diganti dengan memanfaatkan teknologi *QR Code*, dimana admin tidak perlu memasukkan username dan *password* lagi, melainkan cukup dengan mengarahkan *QR Code* ke webcam. Selain itu untuk menambah keamaman maka dibuat tambahan sistem autentukasi dengan cara mengirimkan kode OTP ke

telepon selularadmin yang terdaftar dalam database. Kode OTP yang dikirimkan hanya berlaku untuk sekali sesi login serta hanya berlaku dalam kurun waktu 5 menit saja, sehingga akan menambah sistem keamanan login.

Otentikasi tentu berhubungan erat dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri.Agar dua pihak yang bisa saling berkomunikasi tentu harus saling memperkenalkan diri terlebih dahulu, untuk validasi user pada saat memasuki sistem.Autentikasi merupakan sebuah proses identifikasi yang dilakukan oleh pihak yang satu terhadap pihak yang lain ataupun sebaliknya dengan melakukan berbagai proses identifikasi untuk memastikan keaslian dari informasi yang diterima [1]. Autentikasi adalah suatu langkah untuk menentukan atau memastikan bahwa seseorang (atau sesuatu) adalah autentik atau asli. Melakukan autentikasi terhadap sebuah objek adalah melakukan konfirmasi terhadap kebenarannya. Sedangkan melakukan autentikasi terhadap seseorang biasanya adalah untuk memverifikasi identitasnya. Sedangkan pada suatu sistem komputer, autentikasi umumya terjadi pada saat login atau permintaan akses [6].

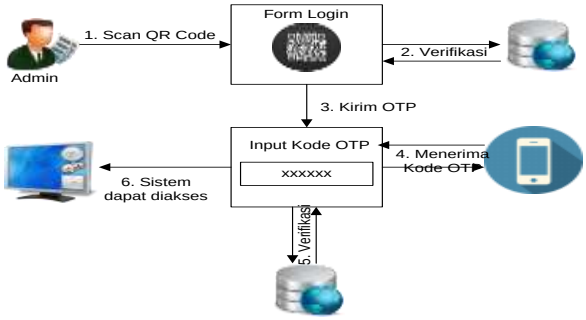
OTP (*One Time Password*) merupakan teknik autentikasi yang hanya berlaku untuk satu kali penggunaan [8]. Kelemahan paling penting yang ditujukan oleh OTP berbeda dengan password statis, OTP tidak rentan terhadap serangan replay (replay attack) [7]. Dalam konteks autentikasi, OTP biasanya digunakan sebagai mekanisme otentikasi tambahan sehingga OTP disebut sebagai dua factor otentikasi (*two-factor-authentication*) [9]. Berikut merupakan metode-metode yang digunakan pada pembangkitan OTP, yaitu sebagai berikut:

a. Berdasarkan sinkronisasi waktu, metode seperti ini digunakan untuk otentikasi antara client dan server karena hanya berlaku untuk waktu yang singkat.
b. Berdasarkan suatu algoritma matematika yang menggunakan masukkan nilai OTP sebelumnya untuk mendapatkan nilai OTP baru.
c. Berdasarkan suatu nilai *challenge* dimana OTP dihasilkan dari suatu algoritma matematika yang mengkombinasikan pengetahuan terhadap nilai rahasia challenge (contoh metode seperti ini diterapkan pada otentikasi untuk suatu transaksi atau counter)

*Quick Response Code* sering di sebut QR Code atau kode QR adalah semacam simbol dua dimensi yang dikembangkan oleh Denso Wave yang merupakan anak perusahaan dari Toyota sebuah perusahaan Jepang pada tahun 1994. Menyampaikan informasi secara cepat dan juga mendapat tanggapan secara cepat adalah merupakan tujuan dari QR Code ini.

Tujuan lain dari penelitian ini adalah untuk mengimplementasikan QR Code yang diterapkan pada mekanisme otentikasi kode OTP dengan menggunakan telepon seluler. Metode yang akan digunakan dalam penelitian ini ialah metode penelitian terapan, dimana hasil dari penelitian tersebut dapat langsung diterapkan untuk memecahkan permasalahan yang ada. Dari tahapan awal aplikasi yaitu melakukan scan QR Code yang sesuai dengan database pada halaman web yang telah di generate sebelumnya. Kemudian sistem akan memverifikasi data QR Code ke dalam database. Jika sesuai (valid) maka kode verifikasi dikirimkan ke nomer telepon melalui SMS. Lalu admin memasukan kode verifikasi ke untuk proses autentikasi ke dalam sistem. Jika tidak sesuai (invalid) maka sistem akan menampilkan pesan kesalahan dan kode OTP tidak akan dikirimkan ke telepon selular admin.

Gambar 1 menjelaskan gambaran umum sistem login pada aplikasi web yang dibangun dengan menerapkan QR Code dan otentikasi kode OTP.

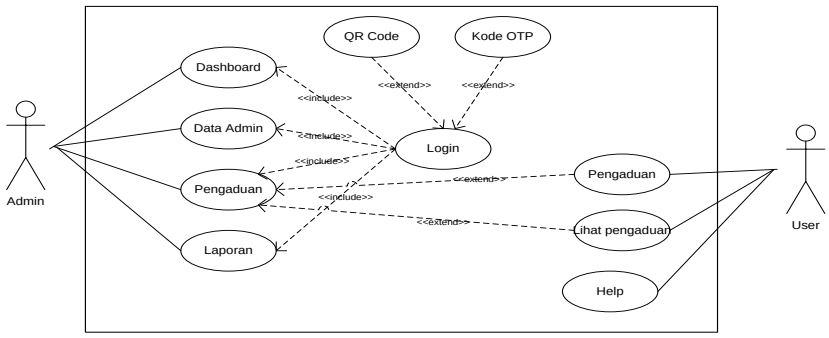



**Gambar 1**. Skema Pengembangan Proses Login

Berdasarkan gambar 1 menjelaskan skema dari pengembangan proses login yang diterapkan pada aplikasi yang dibangun. Untuk dapat mengakses sistem maka admin harus melalui dua tahap verifikasi, pertama admin melakukan scan QR Code dan sistem akan memverifikasi ke dalam database. Selanjutnya sistem akan mngirimkan kode OTP ke telepon selular admin, lalu tahap kedua admin memasukkan kode OTP dan sistem akan memverifikasi kedalam database. Selanjutnya sistem akan dapat diakses jika QR Code dan kode OTP yang dimasukkan benar (valid) dan terdaftar dalam database.

Use case diagram merupakan pemodelan untuk menggambarkan kelakuan dari sistem yang dibuat dan mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem yang dibuat serta digunakan untuk

mengetahui fungsi apa saja yang ada didalam sebuah sistem dan siapa saja yang berhak menggunakan fungsi-fungsi tersebut. Gambar 2 berikut menampilkan use case diagram sistem.




**Gambar 2.** Use Case Diagram Sistem

Sesuai gambar 2 terdapat dua aktor yang terdapat dalam sistem, yaitu admin yang memiliki hak akses untuk login, melihat dashboard, mengelola data admin, mengelola data pengaduan, dan mencetak laporan pengaduan dan user.memiliki hak akses untuk melakukan pengaduan, melihat status pengaduan, dan melihat informasi help.

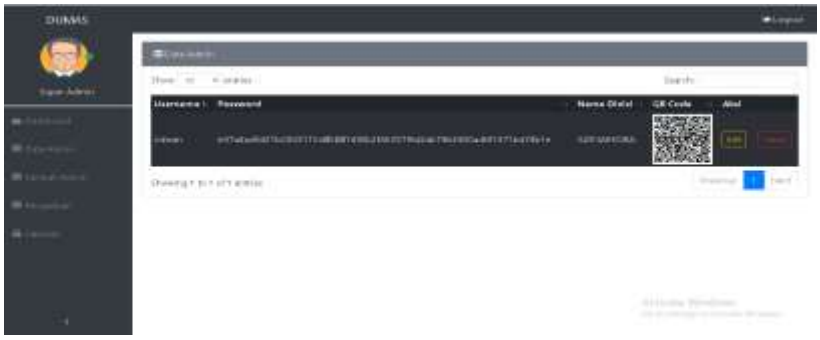
Implementasi sistem merupakan tahapan yang dilakukan setelah perancangan sistem selesai dilakukan dan selanjutnya akan diimplementasikan pada bahasa pemrograman yang akan digunakan.Implementasi sistem dilakukan dengan setiap tampilan antarmuka (interface) yang akan menjelaskan fungsi dari setiap halaman yang terdapat dalam aplikasi.


**Gambar 3**. Implementasi Halaman Login

Halaman login digunakan oleh admin untuk meng-autentikasi diri sebelum masuk ke halaman utama sistem. Gambar 3 memperlihatkan tampilan awal dari halaman login admin, pada halaman ini sistem akan mengaktifkan webcam secara otomastis. Admin harus melakukan scan QR Code ke arah webcam dan sistem akan membaca kode QR Code yang berisi akun admin dan mencoccokkan data kedalam database. Jika terdaftar maka sistem akan mengirimkan kode OTP ke telepon selular admin sesuai dengan yag terdaftar dalam database. Gambar 4 menampilkan implementasi setelah admin melakukan scan QR Code yang terdaftar dalam database.


**Gambar 4**. Proses Input Kode OTP

Gambar 4 memperlihatkan proses penginputan kode OTP untuk proses autentikasi admin dalam mengakses sistem. Kode OTP yang dikirimkan ke telepon selular admin berjumlah 6 (enam) digit angka dan bersipat hanya bisa dipakai satu kali saja serta berlaku hanya dalam kurun waktu selama 5 (lima) menit. Setelah menginputkan kode OTP, selanjutnya pilih tombol Konfirmasi dan sistem akan melakukan verfifiksi kedalam database. Jika kode OTP yang dimasukkan benar (valid), maka sistem akan menampilkan halaman utama sistem (dashboard). Sedangkan jika kode OTP yang dimasukkan salah (invalid), maka sistem akan menmpilkan informasi pesan kesalahan. Jika kode OTP tidak terkirim ke telepon selular maka pilih tombol Kirim Ulang OTP untuk mengirimkan ulang kode OTP.




**Gambar 5.** Implementasi Halaman Data Admin

## 3. KESIMPULAN

Dari hasil pengujian dan implementasi yang sudah dilakukan, didapatkan beberapa kesimpulan yaitu sebagai berikut:

a. Penerapan OTP (One Time Password) dapat mengamankan sistem login website dengan cara mengirimkan kode OTP ke telepon selular admin. Kode OTP yang dikirmkan hanya berlaku untuk satu kali sesi login serta berlaku hanya dalam kurun waktu 5 menit, sehingga kode OTP tidak dapat digunakan kembali pada sesi login berikutnya.
b. Teknologi QR Code dapat dijadikan alternatif untuk mempermudah proses login tanpa harus menginputkan username dan password lagi. Sementara kode OTP digunakan untuk mengatentikaasi admin yang akan menjadikan sistem keamanan login menjadi lebih aman karena hanya berlaku untuk satu kali sesi login.

## DAFTAR PUSTAKA

[1] Azam. M. N. A. (2016). Otentikasi Sistem Dengan Menggunakan One Time Password Memanfaatkan Smartphone Android. Jurnal LINK, Vol. 24, No. 1.
[2] Raharjo. W. S, dkk. (2017). Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login.Jurnal Teknik Informatika dan Sistem Informasi, Vol. 3, No. 1.
[3] Arifin. M, dkk.(2017). Integrasi Login Tanpa Mengetik Passwordpada WordPress.JNTETI, Vol. 6, No. 2.
[4] Sholeh. M. L & Muharom. L. A. (2016). Smart Presensi Menggunakan QR-Code Dengan Enkripsi Vigenere Cipher.Journal of Mathematics and Its Applications, Vol. 13, No. 2.
[5] Paramarta. D. Q. P. A, dkk.(2018). Implementasi Algoritme Advance Encryption Standard (AES) Pada Enkripsi dan Dekripsi QR-Code.Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, Vol. 2, No. 12.
[6]. Suling. C. E, dkk. (2017). Prototype Pengembangan Autentikasi Login Menggunakan Teknologi Quick Respone Code.Seminar Nasional Teknik Elektro dan Informatika (SNTEI) Politeknik Negeri Ujung Pandang.
[7] Ramadhan. M. S & Ariyani. P. F. (2018). Peningkatan Keamanan Login Website Dengan Implementasi One Time Password Menggunakan Algoritma SHA1 Dan MD5 Berbasis Mobile. SKANIKA, Vol 1, No. 2.

[8] Yusuf. R & Anggriawan.E. (2015).Penerapan Metode Smart Authentication Dalam Layanan E-Banking Menggunakan Two Channel Authentication dan QR-Code Pada Perangkat Mobile Android. Seminar Nasional Sistem Informasi Indonesia, Sekolah Tinggi Sandi Negara.
[9] Daqiqil Id. I, dkk. (2016). Implementasi TOTP (Time-Based One Time Password) Untuk Meningkatkan Keamanan Transaksi E-Commerce.Konferensi Nasional Sistem & Informasi Universitas Riau.
[10] Naufal. M & Purwanto.P (2018). Implementasi Keamanan Login Dengan Metode One Time Password (OTP) Menggunakan Fungsi Hash Algoritma SHA-512 Pada SMP Negeri 3 Tangerang Selatan. SKANIKA, Vol 1, No.