JUSTIN
Jurnal Sistem dan Teknologi Informasi
p-ISSN : 2460-3562 / e-ISSN : 2620-8989
DOI: 10.26418/justin.v8i4.42247
Vol. 08, No. 4, Oktober 2020

Implementasi Two Factor Authentication (2FA) pada Sistem Keamanan Otentikasi User di Aplikasi Kasir Legends Barbershop

Gustafi Candra Mahardhika[#1], Felix David[#2]
[#]*Departemen Teknik Informatika, Universitas Kristen Satya Wacana*
Jl. Dr. O. Notohamidjodjo, Blotongan, Sidorejo, Kota Salatiga, 50715
[1]candragustafi@gmail.com
[2]felix@uksw.edu

Abstrak

Memberikan layanan terbaik untuk mencapai kepuasan pelanggan menjadi tujuan utama bagi perusahaan-perusahaan jasa. Untuk itu, perusahaan dituntut memiliki kualitas manajemen yang baik, terutama manajemen keuangan yang baik dengan memanfaatkan teknologi informasi (perangkat lunak/software). Keamanan terhadap akses data keuangan dari orang-orang yang tidak bertanggung jawab merupakan masalah utama yang harus dihadapai oleh perusahaan yang memanfaatkan teknologi informasi. Hal yang sama dirasakan oleh Legends Barbershop dimana akses awal ke data keuangan adalah melalui aplikasi kasir. Oleh sebab itu, perlu adanya suatu mekanisme yang mengatur dan membatasi akses ke data keuangan yang dilakukan melalui aplikasi kasir. Metode Two Factor Authentication (2FA) yang digunakan dalam penelitian ini akan memberikan perlindungan terhadap akses ke perangkat lunak dengan melakukan dua tahap otentikasi. Tahap pertama dengan menggunakan kombinasi username dan password dan tahap kedua dengan mengirimkan serangkaian kode acak ke mobile device (ponsel) pengguna yang sudah terdaftar. Hasil akhir penelitian ini menghasilkan aplikasi tambahan yang akan melakukan otentikasi terhadap pengguna di aplikasi kasir. Pengujian dilakukan menggunakan metode perhitungan skala Likert di lima cabang Legends Barbershop dan diperoleh total indeks keseluruhan sebesar 92%. Nilai indeks menunjukkan bahwa responden setuju dengan adanya tambahan keamanan pada otentikasi user di Aplikasi Kasir Legends Barbershop.

Kata kunci: two factor authentication(2FA), autentikasi, login, keamanan

Implementation of Two Factor Authentication (2FA) on the User Authentic Security System in the Legends Barbershop Cashier Application

Abstract

Providing the best service to achieve customer satisfaction is the main goal for service companies. Therefore, companies are required to have good quality management, especially good financial management by utilizing information technology (software). Security of access to financial data from people who are not responsible is a major problem that must be faced by companies that utilize information technology. The same thing is felt by Legends Barbershop where initial access to financial data is through the cashier application. Therefore, there is a need for a mechanism to regulate and limit access to financial data through the cashier application. The Two Factor Authentication (2FA) method used in this study will protect against access to the software by carrying out two stages of authentication. The first stage uses a username and password combination and the second stage involves sending a series of random codes to the registered user's mobile device (cellphone). The final results of this study produce additional applications that will authenticate users in the cashier application. The test was carried out using the Likert scale calculation method in the five branches of Legends Barbershop and the total index was 92%. The index value shows that the respondent agrees with the added security of user authentication in the Barbershop Legends Cashier Application.

Keywords: Two Factor Authentication (2FA), Authentication, Login, Security

I. PENDAHULUAN

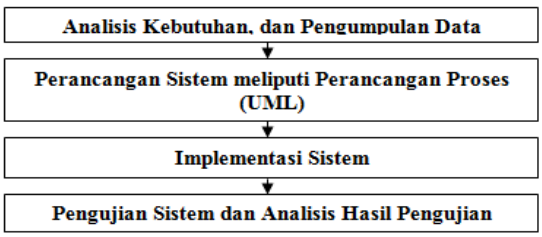
Saat ini perkembangan perangkat lunak dengan dukungan internet sangat pesat, segala pekerjaan dapat dibantu dengan perangkat lunak untuk menjalankan proses bisnis yang ada, seperti halnya proses transaksi, pembukuan dan pengecekan pemasukan keuangan sebuah perusahaan. Keuntungan utama bagi perusahaan dengan beberapa cabang yang tersebar di beberapa kota adalah memudahkan pimpinan perusahaan dalam melakukan cek pembukuan pada setiap cabang tanpa harus hadir secara fisik di perusahaan cabang tersebut[1].

Legends Barbershop adalah sebuah usaha potong rambut pria yang memiliki cabang tersebar di beberapa kota yaitu Salatiga, Kudus, Ungaran, Pati dan Jepara, sehingga dibutuhkan pengelolaan sistem manajemen keuangan yang baik dengan bantuan sistem informasi. Keamanan data dari penggunaan sistem informasi ini menjadi prioritas utama bagi *stakeholder*, terutama pada aplikasi kasir yang merupakan pintu akses ke data keuangan. Penggunaan user name dan password yang selama ini digunakan dirasa kurang memberikan rasa aman bagi *stakeholder* [2]. Oleh sebab itu perlu adanya fitur tambahan pada aplikasi kasir sehingga perlndungan akses data melalui aplikasi kasir dapat dilakukan. Pada proses *login*, dimana *password* akan menjadi *single point of attack* untuk mengakses aplikasi, perlu ditambahkan proteksi lanjutan untuk mengamankan aplikasi [3]. Disinilah peran metode ***Two Factor Authentication*** (2FA), sebagai proteksi tingkat lanjut untuk mengamankan akses aplikasi. 2FA memberikan dua langkah otentikasi saat pengguna mengakses aplikasi kasir, langkah pertama dengan menggunakan user name dan password dan langkah kedua dengan menggunakan kode acak unik [4].

Tujuan penelitian ini adalah membangun aplikasi lanjutan untuk keamanan akses aplikasi kasir dan untuk mengetahui tanggapan penggunan dari aplikasi tersebut lanjutan tersebut.

II. METODOLOGI

Dalam penelitian ini, ada beberapa langkah yang harus dilakukan secara tersruktur agar sesuai dengan tujuan. Tahapan penelitian yang digunakan dapat dilihat pada Gambar 1.



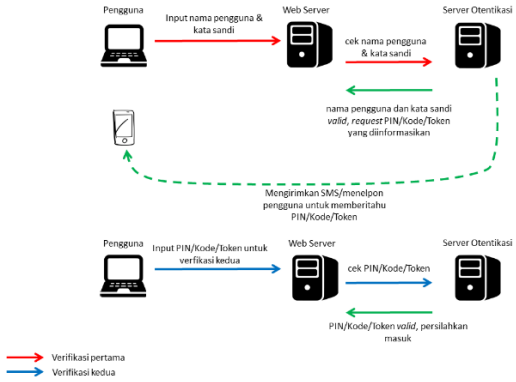
Gambar 1. Tahapan penelitian

A. *Analisis Kebutuhan dan Pengumpulan Data*

Tahap pertama yaitu menganalisis kebutuhan dan pengumpulan data. Tahap ini merupakan tahap awal untuk mengetahui kebutuhan-kebutuhan yang diperlukan dalam merancang sebuah sistem. Fokus pertama yang harus dilakukan ialah menganalisis tujuan bisnis perusahaan. Tujuan bisnis perusahaan diperlukan untuk memahami kendala yang kemungkinan terjadi dalam penelitian ini dan mengetahui kemampuan menjalankan hasil penelitian sesuai dengan kebutuhan. Tahapan ini dilakukan dengan cara melakukan wawancara kepada pihak pemilik usaha Legends Barbershop.

B. *Perancangan Sistem*

Pada tahap ini menggunakan metode *Prototyping* dalam melakukan perancangan sistem informasi. *Prototyping* model adalah metode yang digunakan untuk mendefinisikan serangkaian sasaran umum bagi perangkat lunak serta mengidentifikasikan kebutuhan *input*, pemrosesan, ataupun *output* detail [5]. Perancangan sistem nantinya akan meliputi alur program dengan menggunakan UML (*Unified Modeling Language*). Diagram UML akan meliputi diagram *use case*, diagram *activity* dan diagram *sequence*. UML yang telah dibuat nantinya akan dilanjutkan dengan mengimplementasikannya. Tahapan yang terakhir pada metode *prototyping* adalah evaluasi *prototype* [6].



Gambar 2. Rancangan proses aplikasi kasir legends barbershop

Pada Gambar 2 merupakan alur proses aplikasi kasir Legends Barbershop. Pengguna akan diminta memasukan *username* dan *password*, lalu *username* dan *password* tersebut akan di cek apakah sudah terdaftar. Jika sudah maka sistem akan mengirimkan kode verifikasi. kode verifikasi tersebut dimasukan ke aplikasi untuk dapat melanjutkan proses login. Jika sesuai maka pengguna dapat langsung menggunakan aplikasi tersebut [7].

C. *Implementasi Sistem*

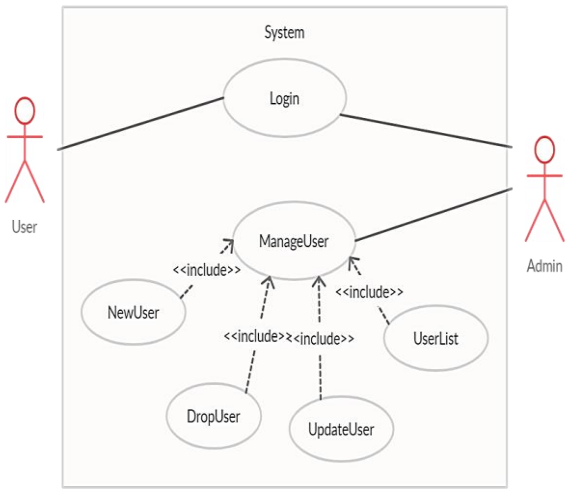
Tahap ketiga yaitu Implementasi Sistem. Pada tahap ini dilakukan implementasi berdasarkan hasil yang didapat dari analisa kebutuhan dan pengumpulan data kemudian diimplementasikan dengan dasar dari perancangan sistem.

D. *Pengujian Sistem*

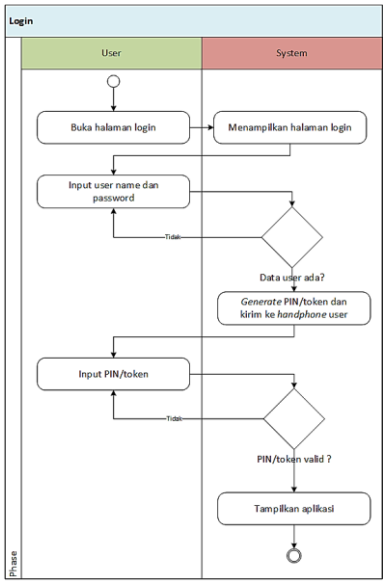
Tahap keempat adalah pengujian sistem dan analisis hasil pengujian. Pengujian aplikasi atau evaluasi *Prototype* dilakukan untuk memastikan apakah fungsi-fungsi didalam sistem sudah berjalan dengan baik atau belum.

III. HASIL DAN PEMBAHASAN

Gambar 3 merupakan diagram *use case* untuk melakukan proses Login dan pengelolaan user. Terdapat dua aktor, yaitu User dan Admin. Admin dapat melakukan proses pengelolaan user yang diijinkan untuk mengakses aplikasi melalui mekanisme Login. Pendaftaran nomor ponsel yang akan digunakan oleh user untuk menerima kode login yang akan dikirimkan oleh sistem dilakukan pada saat Admin mendaftarkan user baru ke dalam sistem [8].

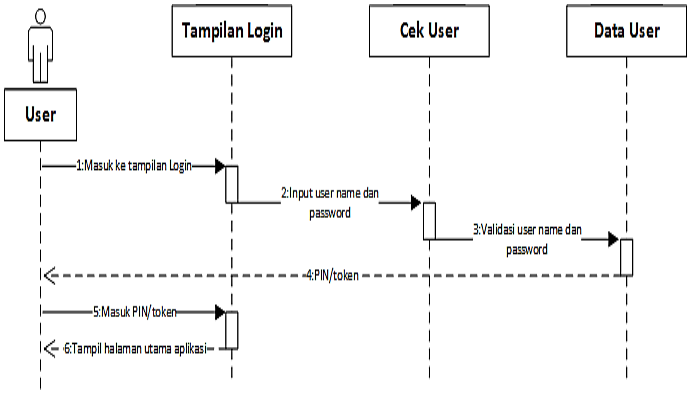


Gambar 3. Diagram *use case* proses Login



Gambar 4. Diagram *activity* proses Login

Gambar 4 merupakan *activity diagram* dari proses Login. Dimulai pada saat user mengakses halaman login, kemudian dilanjutkan dengan menginputkan user name dan password user bersangkutan [9]. Sistem kemudian akan melakukan validasi terhadap data user name dan password yang diinputkan. Jika validasi berhasil dilakukan user, artinya data user name dan password ada dan sesuai dengan data yang ada di dalam basis data sistem maka system secara otomatis akan membuat PIN/token yang akan dikirmkan ke ponsel user yang sudah terdaftar. User kemudian akan memasukkan PIN/token tersebut pada tampilan yang tersedia.



Gambar 5. Diagram *sequence* proses Login

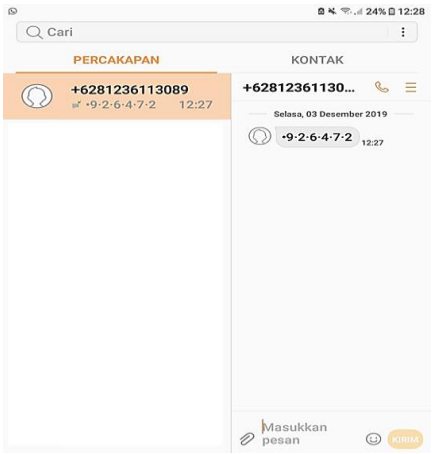
Gambar 5 merupakan diagram sequence dari proses Login yang dilakukan user. PIN/token akan secara otomatis akan dibuat oleh system Ketika user name dan password yang diberikan user telah berhasil divalidasi oleh sistem.

Gambar 6. Tampilan Login Aplikasi Kasir

Gambar 6 merupakan tampilan login dari Aplikasi Kasir. U*sername* dan *password* yang diinputkan harus sudah terdaftar oleh admin ke dalam basis data. *Username* dan *password* yang digunakan bersifat *case sensitive* dan dapat berupa huruf, angka, atau kombinasi keduanya, sehingga memudahkan pengguna untuk mengingatnya. *Password* memiliki keamanan tingkat pertama karna huruf atau angka yang di masukan akan otomatis berubah menjadi simbol sehingga tidak akan terlihat oleh pengguna maupun orang lain. Dengan kata lain harus pemilik *username* dan *password* yang bisa *login* [10].

Gambar 7 merupakan tampilan untuk melakukan inputan PIN/token yang di dapat melalui *Short Message Service* (SMS) di ponsel user [11]. Jangka waktu yang diberikan untuk memasukan kode verifikasi hanya enam puluh detik. Jika melebihi batas tersebut maka sistem akan keluar otomatis kembali ke tampilan *login* seperti Gambar 7. SMS yang didapat berupa *random code* untuk verifikasi aplikasi, seperti yang tampak pada Gambar 8. SMS dikirim langsung ke nomor ponsel pengguna oleh sistem, sehingga memudahkan pengguna untuk menerima langsung kode tersebut demi menjaga sifat kerahasiaan kode yang dikirim [12],[13].

Gambar 7. Tampilan input PIN/token



Gambar 8. SMS PIN/token aplikasi

Gambar 9. Tampilan Utama Aplikasi Kasir Legends Barbershop

Gambar 9 merupakan tampilan utama aplikasi kasir Legends Barbershop. Aplikasi tersebut akan otomatis *logout* ketika tidak digunakan selama enam puluh detik dan kembali ke tampilan *login* seperti pada Gambar 6 [14].

Pengujian Aplikasi Kasir Legends Barbershop, dilakukan dengan menggunakan skala *likert* dimana data hasil pengujian dikumpulkan melalui kuisioner yang dibagikan kepada responden. Responden dalam pengujian ini melibatkan enam lokasi Legends Barbershop yang ada di Salatiga (2 cabang), Kudus (1 cabang), Ungaran (pusat), Pati (1 cabang) dan Jepara (1 cabang), untuk memperoleh hasil yang subjektif. Pertama-tama, responden (dalam hal ini adalah user kasir) akan ditunjukkan bagaimana cara menggunakan aplikasi. Setelah itu, user akan melakukan percobaan sendiri untuk mendapatkan pengalaman terhadap proses login. Standar penilaian yang digunakan dalam pengujian ini, disajikan pada Tabel I, sebagaimana dalam [15].

TABEL I
PARAMETER NILAI

Skor	Nilai
1	Sangat Tidak Setuju
2	Tidak Setuju
3	Netral
4	Setuju
5	Sangat Tidak Setuju

TABEL II
HASIL PENGUJIAN

No	Pertanyaan	Jawaban Responden					Jum	Idx (%)
		Ax 1	Ax 2	Ax 3	Ax 4	Ax 5		
User Interface								
1	Apakah tampilan login dalam aplikasi mudah dipahami ?	0	0	0	1	4	24	96
2	Apakah aplikasi login mudah dioperasikan ?	0	0	0	2	3	23	92
Total:		0	0	0	3	7	47	31.3
Fungsionalitas								
1	Apakah proses login bisa dilakukan?	0	0	0	1	4	24	96
2	Apakah user menerima PIN yang dibutuhkan?	0	0	0	0	5	25	100
3	Apakah aplikasi bermanfaat?	0	0	0	0	5	25	100
4	Apakah aplikasi ini sesuai dengan kebutuhan ?	0	0	0	0	5	25	100
5	Apakah proses login lebih cepat?	0	3	2	0	0	12	4
6	Apakah aplikasi lebih aman?	0	0	0	0	5	25	100
7	Apakah aplikasi komunikatif?	0	0	0	1	4	24	96
Total:		0	3	2	1	14	86	43
Total Keseluruhan Indeks:							**23**	**92**

Berdasarkan hasil pengujian yang tersaji pada Tabel II, untuk kelompok pertanyaan pertama yang berhubungan dengan kriteria User Interface, diperoleh indeks sebesar 31.3%. Sedangkan kelompok pertanyaan kedua untuk kriteria Fungsionalitas, diperoleh indeks sebesar 43%. Pada pertanyaan kelima di kriteria Fungsionalitas, respon dari responden terhadap adanya peningkatan mekanisme

keamanan dengan 2FA ini merupakan suatu hal yang wajar dan sudah diperkirakan oleh penulis. Sebab antara keamanan dan kenyamanan akan selalu berbanding terbalik jika dibandingkan.

Total keseluruhan indeks untuk kedua kriteria yang diujikan adalah sebesar 92%. Nilai indeks ini dapat disimpulkan bahwa responden yang mewakili lima cabang Legends Barbershop setuju dengan pemanfaatan Two Factor Authentication (2FA) sebagai tambahan keamanan pada otentikasi user di Aplikasi Kasir Legends Barbershop.

IV. KESIMPULAN

Berdasarkan hasil peneltian yang telah dilakukan dapat disimpulkan bahwa pembangunan aplikasi lanjutan untuk keamanan akses aplikasi kasir dengan menggunakan Two Factor Authentication (2FA) dapat diimplemntasikan. Secara keseluruhan, pengguna menunjukkan tanggapan yang baik terhadap aplikasi lanjutan ini. Dengan menggunakan skala likert pada pengujian, diperoleh total indeks keseluruhan dari dua kriteria yaitu User Interface dan Fungsionalitas yaitu sebesar 92%. Ini menunjukkan bahwa peningkatan keamanan akses ke aplikasi Kasir mampu memenuhi kebutuhan pengguna, dalam hal ini adalah *stakeholder* dari Legends Barbershop.

Penelitian lanjutan yang dapat dilakukan dari penelitan ini adalah pengembangan mekanisme pengiriman PIN/token (On Time Password = OTP) yang tidak menggunakan teknologi *short message service* (SMS). Penggunaan SMS memang lebih sederhana tetapi sangat tergantung dengan ketersediaan jumlah pulsa yang harus tersedia di mesin server pengirim PIN/token-nya. Pengembangan dapat dilakukan dengan menggunakan teknologi yang lebih baru, seperti menggunakan aplikasi WhatsApp atau Telegram.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Tuhan Yang Maha Esa atas rahmat dan penyertaanNya sehingga penulis dapat menyelesaikan penelitian ini.

DAFTAR PUSTAKA

[1] Priambodo, Y. D., & Wongso, O., "Sistem Inventori Dan Manejemen Kebutuhan Dalam Berbelanja", 2019, Jurnal Strategi, 217-226.

[2] Chen, Alex. Q & Goh, Weihan., "*Two Factor Authentication Made Easy"*, ICWE, Springer International Publishing, 2015.

[3] Stanislav, Mark., "*Two-Factor Authentication"*, O'Reilly, 2015.

[4] A. Amin, I. ul Haq, and M. Nazir, "Two-Factor authentication," Int. J. Comput. Sci. Mob. Comput., vol. 6, no. 7, pp. 5–8, 2017.

[5] S. Biswas and S. Biswas, "Password security system with 2-way authentication," 2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Kolkata, 2017, pp. 349-353, doi: 10.1109/ICRCICN.2017.8234533.

[6] Karuana, S., "Aplikasi Pemeriksaan Sasaran Operasi P2TL Dengan Metode Rapid Application Development Berbasis Android Web Service dengan Arsitektur Komunikasi Restful API pada PT PLN WS2JB", 2018, Tugas Akhir Program Studi Manajemen Informatika Politeknik Negeri Sriwijaya, Palembang.

[7] Kurniawan, M. B., & Fatimah, T., "Aplikasi Nilai Online Menggunakan One Time Password Dengan Algoritma SHA 512 Berbasis Web pada SMP PGRI 336", 2018, SKANIKA, 411-416.

[8] Nama, G. F., & Muludi, K., "Implementation of Two Factor Authentication (2FA) to Encgance the Security of Academic Information System", 2018, Journal Of Engineering and Applied Sciences, 2209-220.

[9] Kurniawan, Y., Oslan, Y., & Kristanto, H., "Implementasi Rest-Api Untuk Portal Akademik UKDW Berbasis Android", 2013, Jurnal Eksplorasi Karya Sistem Informasi dan Sains, Vol 6, No 2.

[10] W. Sudiarto Raharjo, I. D. E.K. Ratri, and H. Susilo, "Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login," J. Tek. Inform. dan Sist. Inf., vol. 3, no. 1, pp. 127–136, 2017, doi: 10.28932/jutisi.v3i1.579

[11] Alharbi, E., & Alghazzawi, D., "Two Factor Authentication Framework Using OTP-SMS Based on Blockchain. Transactions on Machine Learning and Artificial Intelligence", vol. 7, no. 3, 17-27, 2019, https://doi.org/10.14738/tmlai.73.6524

[12] Z. Khalid, P. Paul, S. P. Chattopadhyay and A. N. Biswas, "Secure authentication with dynamic password," 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, 2016, pp. 1-7, doi: 10.1109/IEMCON.2016.7746081.

[13] E. E. N. and S. Nivetha, "Design of a two-factor authentication ticketing system for transit applications," 2016 IEEE Region 10 Conference (TENCON), Singapore, 2016, pp. 2496-2502, doi: 10.1109/TENCON.2016.7848483.

[14] Wang, Ding & Wang, Ping., "Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound", IEEE Transactions on Dependable and Secure Computing, 2016, PP. 1-22. 10.1109/TDSC.2016.2605087.

[15] Nazir, M.m "Metode Penelitian". Ghalia Indonesia. Jakarta, 2014.

[16] J. Zhang, X. Tan, X. Wang, A. Yan and Z. Qin, "T2FA: Transparent Two-Factor Authentication," in IEEE Access, vol. 6, pp. 32677-32686, 2018, doi: 10.1109/ACCESS.2018.2844548.