e-ISSN 2549-7472
Edumatic: Jurnal Pendidikan Informatika
Vol. 4 No. 1, Juni, 2020, **Hal. 111-120**
DOI: 10.29408/edumatic.v4i1.2158

Implementasi One Time Password Menggunakan Algoritma SHA-512 Pada Aplikasi Penagihan Hutang PT. XHT

Rizki[1], Sri Mulyati[2]
[1,2] Program Studi Teknologi Informasi, Universitas Budi Luhur
email: 1611510296@student.budiluhur.ac.id[1], sri.mulyati@budiluhur.ac.id[2]

(Received: 28 Mei 2020/Accepted: 8 Juni 2020 / Published Online: 20 Juni 2020)

Abstrak

PT. XHT adalah salah satu perusahaan swasta bergerak di bidang penagihan hutang. Perusahaan ini memiliki sistem penagihan hutang berbasis web. Namun, pernah terjadi pencurian *username* dan *password* pada sistem berjalan. Hal ini disebabkan banyak hal, diantaranya *password* yang terlalu mudah. Salah satu solusi mengatasi hal ini adalah dengan meningkatkan keamanan autentikasi, yaitu dibuat sistem *One Time Password.* Pada penelitian ini dibuat sistem keamanan *login One Time Password* menggunakan fungsi hash SHA-512. Dalam mengembangkan sistem ini menggunakan metode *Waterfall Development* sebagai siklus hidup pengembangan perangkat lunak. *One Time Password* sebuah kode acak hanya dapat digunakan satu kali. Pengujian melibatkan beberapa pihak, diantaranya Ahli Media dan Ahli Materi, serta menggunakan metode *black box*. Hasil uji *black box* menunjukkan kelayakan fungsi button berupa masukan dan keluaran. Sementara itu, hasil uji oleh Ahli Media mendapat nilai 82%, sedangkan Ahli Materi adalah 75%. Sehigga dapat disimpulkan bahwa sistem *login One Time Password* menggunakan SHA-512 layak digunakan untuk keamanan pengguna.

Kata kunci: Algoritma SHA-512, Aplikasi Penagihan Hutang, *One Time Password*, *Waterfall*

Abstract

PT. XHT is a private company engaged in debt collection. This company has a web-based debt collection system. However, there has been a theft of usernames and passwords on the running system. This is due to many things, including passwords that are too easy. One solution to overcome this is to increase authentication security, which is a One-Time Password system. In this research, login security system is created using the SHA-512 hash function. In build this system using the Waterfall method as the life cycle of software development (SDLC). This system is a random code can only be used once. The test involved several parties, including Media Expert and Material Expert, and using the black box method. Black box test results indicate the feasibility of the function from the input and output buttons. Meanwhile, the results from the test by the Media Expert scored 82%, while the Material Expert was 75%. So it can be concluded that the One-Time Password login system using SHA-512 is suitable for user security.

Keywords: *Algoritma SHA-512, Debt Billing Application, One Time Password, Waterfall*

PENDAHULUAN

Pada era globalisasi seperti saat ini, kehadiran teknologi informasi sangat berperan penting dalam perubahan di dunia. Perkembangan ini juga mempengaruhi di berbagai bidang, seperti; pertanian, perindustrian, pemerintahan, kesehatan, dan pendidikan. Manusia sebagai pengguna teknologi harus mampu memanfaatkan teknologi informasi yang ada saat ini, maupun perkembangan teknologi informasi tersebut selanjutnya. Tanpa di sadari, penggunaan teknologi informasi telah banyak membantu manusia untuk menyelesaikan pekerjaannya. Oleh karena itu, penggunaan teknologi informasi tersebut baru dapat dirasakan

manfaatnya jika diberikan kepada orang yang tepat, sehingga informasi juga harus relevan terhadap penggunanya (Kinarwanto, 2016).

PT. XHT adalah salah satu perusahaan swasta yang memanfaatkan teknologi informasi bergerak dibidang penagihan hutang. Penagihan hutang di perusahaan ini menggunakan aplikasi berbasis web yang dilakukan oleh seorang *user*. Sebelum masuk ke dalam sistem, *user* di haruskan melakukan *login* terlebih dahulu dengan memasukkan *username* dan *password* (Khairina, 2011). Setelah berhasil, barulah user bisa melakukan penagih hutang kepada pihak *client* yang memiliki tagihan. Permasalahan mulai muncul saat salah satu *user* tidak hadir atau tidak bisa melakukan penagihan. *User* lain tentu sangat mudah melakukan *login* dengan menggunakan *username* dan *password user* tersebut. Hal ini di akibatkan karena keamanan a*ccount* sesama *user* yang sangat rentan dan kurangnya ke waspadaan user dalam menggunakan *username* dan *password*. Selain itu *user* lain yang berhasil *login* dan bukan menggunakan *account* nya, dapat melihat dan mengakses seluruh data *client* tersebut.

Berdasarkan paparan masalah tersebut, maka perlu di kembangkan keamanan sistem *login* yang dapat mengamankan *account user*. Ada beberapa ide pengembangan yang dilakukan, salah satunya token. *Password* pelapis kedua ini lebih banyak di kenal dengan *One Time Password* (OTP). Setelah sebuah *password* dipakai , maka *password* yang sama tidak dapat dipakai untuk kedua kalinya. *Password* tersebut sebuah kode acak yang selalu berubah dan hanya bisa dipakai satu kali. Kode acak di dapat dengan menggunakan algoritme SHA – 512 sebagai pembangkit kode OTP . Pembangkit kode OTP berjalan setelah *user* memasukkan *username, password* dan waktu saat melakukan *login*. Pegiriman kode OTP ada yang melalui SMS, Email atau aplikasi android.

Algoritme SHA-512 termasuk jenis fungsi *hash* yang merupakan pengembangan dari algoritme SHA-1. Fungsi *hash* adalah fungsi yang menerima masukan *string* yang panjangnya sembarang dan mengkonversinya menjadi *string* keluaran yang panjangnya tetap (*fixed*) (Adilah et al., 2017; Sakti et al., 2016). Algoritma SHA – 512 panjang nilai hash yang dihasilkan adalah 512 bit sebagai fungsi *hash* mempunyai sifat-sifat seperti : 1) Sifat *requirement*, h mudah dihitung bila diberikan M. Jika h sukar dihitung, maka tidak dapat menggunakan fungsi hash. 2) Sifat *oneway function*, mudah menghitung h dan sukar mengembalikan nilai M. Tanpa sifat tersebut mudah menemukan nilai keduanya. 3) Sifat *collision free,* mencegah kemungkinan pemalsuan. Tidak mungkin mencari M dan M' sehingga H(M)=H(M') (Mulya, 2009; Sugiyatno & Atika, 2018). algoritma SHA – 512 sebagai pembangkit kode OTP untuk keamanan sistem *login*. Kode OTP ini oleh sistem akan di kirimkan ke *user* melalui SMS yang berguna untuk meng – otentikasi apakah *user* yang melakukan *login* benar – benar dirinya (Kurniawan & Fatimah, 2018; Naufal & Purwanto, 2018; Yahya & Amini, 2018). Otentikasi ini akan dicocokkan dengan yang ada pada sistem (Al Azam, 2016). Namun SMS memiliki *delay* atau jeda waktu yang lama dalam proses pengirimannya dan berbayar.

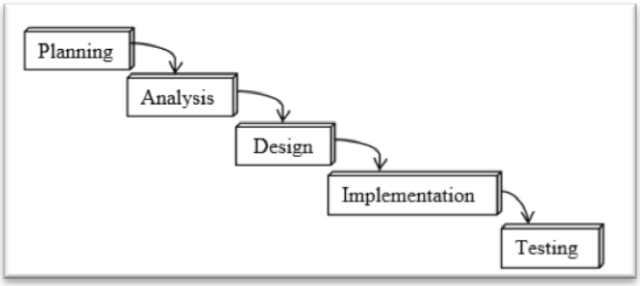
Beberapa peneliti telah menggunakan Arduino Uno dan Arduino Mega untuk keamanan rumah (Dewy, 2018; Saptohadi et al., 2018; Wadhwani et al., 2018; Wijaya et al., 2017). Implementasi *Internet of Things* (IoT) untuk keamanan rumah ini berfungsi jika pemilik terkoneksi dengan internet atau *bluetooth* serta dapat mengontrol atau memonitoring rumah. *Password* atau perintah keamanan ini akan di kirimkan melalui SMS atau aplikasi yang telah di buat oleh peneliti dan hanya bisa digunakan pada saat itu. Pada penilitian yang telah di lakukan tersebut, tidak dijelaskan algoritma apa yang digunakan.

Berdasarkan uraian di atas, penelitian ini mengembangkan keamanan sistem *login One Time Password* dengan menggunakan Algoritma SHA-512 sebagai pembangkit kode *OTP* pada aplikasi penagihan hutang di PT. XHT. Keamanan sistem *login* yang penting dan utama untuk mengamankan *account user* agar dapat meng-auntentikasi apakah *user* yang menggunakan di aplikasi tersebut adalah benar – benar diri nya. Kode OTP akan dikirimkan

melalui aplikasi android sehingga dapat menjaga keamanan *account user* dari *user* lain yang tidak berkepentingan.

METODE

Metode yang digunakan untuk membuat atau mengembangkan sistem ini adalah metode *Waterfall Development*. Pemilihan metode pengembangan sistem berdasarkan kesesuaian model untuk dipakai, dalam metode *waterfall* setiap tahapan-tahapan saling memiliki keterkaitan dan pengaruh (lihat gambar 1). Metode *waterfall* dimulai dari tahap *Planning, Analysis, Design, Implementation, Testing, Maintenance* (Pressman, 2003).



Gambar 1. Metode *Waterfall*

Tahapan *Planning* atau rencana, digunakan untuk pendefinisian tujuan, melakukan uji kelayakan teknis yang berupa ketersediaan *hardware* dan *software*, uji kelayakan operasional yang dimaksud untuk menguji kemampuan *user* yang akan bekerja dalam mengimplementasikan aplikasi, uji kelayakan organisasi untuk menilai kesiapan perusahaan untuk mengembangkan sistem yang akan diterapkan. Tahapan *Analysis* atau analisa ini dilakukan untuk menganalisis kebutuhan-kebutuhan yang diperlukan untuk membangun metode *One Time Password (OTP)* pada sistem penagihan hutang di PT. XHT yang didapatkan dari data kualitatif dan data kuantitatif. Data kualitatif di peroleh dari ahli media dan ahli materi berupa saran dan masukan dalam pengembangan aplikasi. Data kuantitatif di peroleh dari ahli media dan ahli materi berupa penilaian kualitas aplikasi. Nilai parameter ini memiliki rentang untuk mengetahui kelayakan pada suatu sistem. Rentang nilai dapat di lihat pada tabel 1. Tahapan *Design* atau model ini dilakukan untuk menerjemahkan kebutuhan yang sudah dianalisa ke sebuah perancangan perangkat lunak, tahap desain meliputi perancangan struktur data, perancangan struktur sistem, perancangan masukan dan keluaran. Tahap *Implementasi* atau pelaksanaan merupakan tahapan secara nyata dalam mengerjakan suatu sistem yang berguna untuk menerjemahkan desain yang telah dibuat kedalam bahasa pemrograman. Bahasa pemrograman PHP dan PostgreSql sebagai database, merupakan salah satu yang dapat dimengerti oleh komputer. Tahap akhir dilakukan uji untuk memastikan perangkat lunak dapat bekerja sesuai apa yang telah direncanakan, dan digunakan untuk menemukan kesalah dan memastikan sistem akan memberikan hasil yang diinginkan oleh *user*. Dalam tahap *Testing* atau pengujian ini, peneliti menggunakan *black box* untuk mengetahui apakah *software* yang dibuat telah sesuai dengan desainnya dan apakah masih terdapat kesalahan atau tidak, dengan dilakukan penggabungan modul-modul yang telah dibuat.

Tabel 1. Nilai Parameter Kelayakan

No	Persentasi	Kategori
1.	76% - 100%	Sangat Layak
2.	51% - 75%	Layak
3.	26% - 50%	Cukup

4.	0% - 25%	Kurang Layak

HASIL DAN PEMBAHASAN

Hasil

Penelitian ini menghasilkan tampilan *form* implementasi One Time Password (OTP) untuk keamanan *login* berbasis web pada aplikasi penagihan hutang di PT. XHT dengan menggunakan metode *Waterfall*. Adapun langkah – langkah dalam pengembangan dan pelaksanaan metode ini sebanyak 5 langkah yaitu: *Planning, Analysis, Design, Implementation, Testing, Maintenance*.

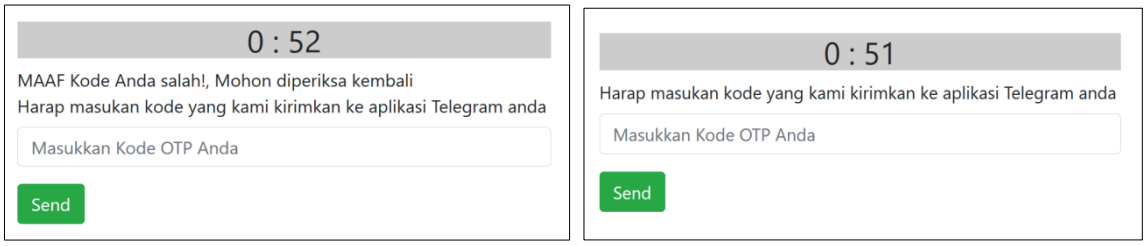
1. Tampilan *Login User*

Login User adalah tampilan pertama kali saat aplikasi di jalankan. Pada tampilan ini terdapat dua buah *textarea* yang berguna setelah memasukkan *username* dan *password* untuk *user*. Terdapat satu buah tombol *button* yang berfungsi untuk *login* (lihat gambar 2).

Gambar 2. Tampilan *Login User*

2. Tampilan Input Kode OTP

Input Kode OTP adalah tampilan setelah *user* berhasil login. Pada tampilan ini terdapat satu buah *text area* yang berguna setelah memasukkan kode OTP yang di kirimkan melalui aplikasi android. Di sini juga terdapat *timer* untuk menghitung batas waktu penginputan kode OTP. Jika *user* salah menginput kode, maka akan di minta untuk menginput ulang kembali. Terdapat satu buah tombol *button send* yang berfungsi untuk mengirim kode OTP, seperti yang terlihat pada gambar 3.



Gambar 3. Tampilan Input Kode OTP

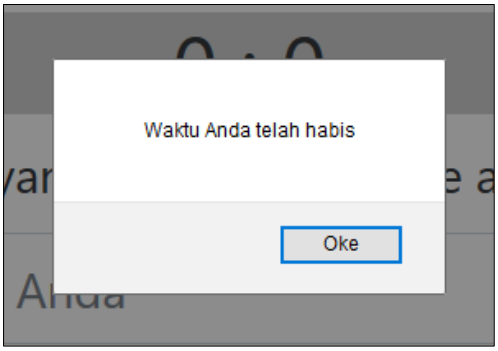
3. Tampilan Kode OTP Pada Aplikasi Android

Kode OTP Pada Aplikasi Android adalah tampilan yang ada pada aplikasi android user untuk menerima kode OTP. Aplikasi ini hanya berfungsi mengetahui kode OTP masing – masing *user* (lihat gambar 4).

4. Tampilan *Time Out* Kode OTP

Time Out Kode OTP adalah tampilan jika *user* terlalu lama memasukkan kode OTP. Pada tampilan ini akan muncul *pop up* yang memberi info kepada *user* bahwa waktu penginputan telah habis. Terdapat satu buah tombol *button* seperti pada gambar 5.

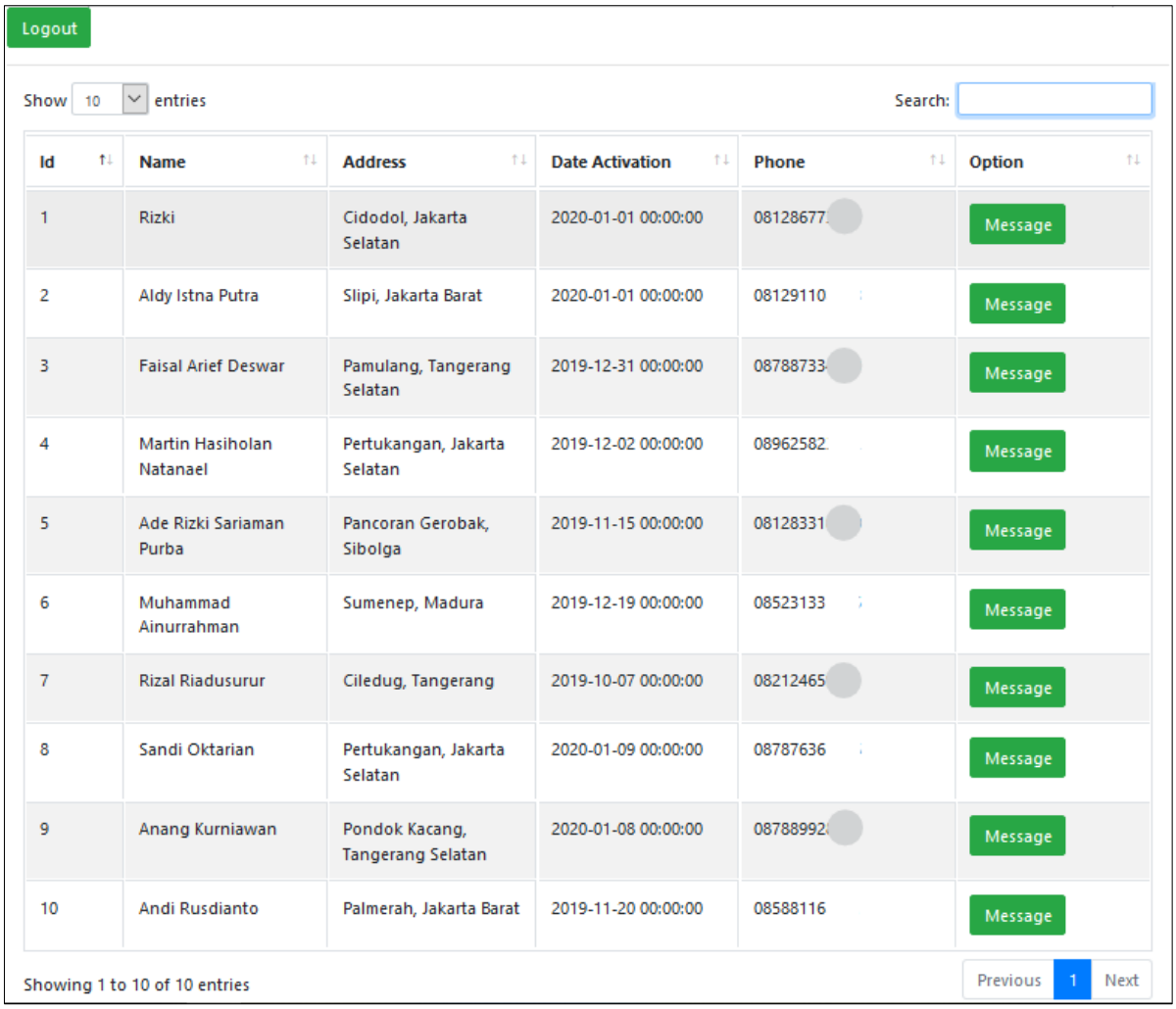
Gambar 4. Tampilan Kode OTP Aplikasi Android



Gambar 5. Tampilan Time Out Kode OTP

5. Tampilan Menu Utama

Tampilan Menu Utama adalah tampilan menu utama *user* setelah berhasil login dan berhasil validasi kode OTP. Di tampilan ini *user* dapat melihat data *client* yang memiliki pinjaman di PT.XHT. Terdapat satu buah tombol *button* yang berfungsi untuk *logout*. Seperti pada gambar 6.



Gambar 6. Tampilan Menu Utama

Hasil Uji

Tahap ini bertujuan untuk mengetahui kelayakan pengembangan aplikasi yang di kembangkan oleh peneliti. Tahap ini berguna untuk mengetahui kesalahan yang ada pada sistem dan memperbaikinya. Pengujian di lakukan oleh peneliti sebelum merealisasikan nya ke perusahaan. Penelitian melalukan beberapa pengecekan fungsi *button* pada sistem yang terkoneksi pada database dan dapat di lihat pada tabel 2-4.

1. *Black box login user*

*Black box login user*berguna untuk menjelaskan *button* yang berfungsi di tampilan layar *form login user*, seperti yang terlihat pada tabel 2.

Tabel 2. *Black Box Form Login User*

Button	**Hasil uji yang diharapkan**	**Hasil**
Login	a) Salah satu *username* dan *password* tidak di isi, akan di minta *login* kembali.	✓
	b) *Username* dan *password* tidak sesuai dengan isi di database, akan di minta *login* kembali.	✓
	c) *Username* dan *password* sesuai dengan isi di database, akan masuk ke *form* input kode OTP.	✓

Keterangan :

Jika *username* atau *password* tidak di isi dan *buttonlogin* di klik, maka akan di minta untuk inputkembali.Jika *username* dan *password* tidak ada di dalam databasedan *button login*di klik, maka akan di minta untuk input kembali.

Jika *username* dan *password*yang di input ada di dalam database dan *button login*di klik, maka akan masuk ke dalam tampilan *form* input kode OTP.

2. *Black box input kode* OTP

Black box input kode otp berguna untuk menjelaskan *button* yang berfungi di tampilan *form* input kode OTP (lihat tabel 3).

Tabel 3. *Black Box Form* Input Kode OTP

Button	**Hasil uji yang di harapkan**	**Hasil**
Send	a) Kode OTP yang di input tidak sesuai dengan sistem, akan di minta input kembali.	✓
	b) Kode OTP yan di input sesuai dengann sistem, akan masuk ke *form* tampilan menu utama.	✓
Oke	Batas waktu input kode telah habis, akan di minta *login* kembali.	✓

Keterangan :

Jika kode OTP yang di input tidak ada di dalam database dan *button send* di klik, maka akan di minta kembali untuk menginput kode OTP.

Jika kode OTP yang di input ada di dalam database dan *button send* di klik, maka akan masuk ke dalam tampilan menu utama.

Jika *user* terlalu lama menginput kode OTP sesui dengan batas waktu yang di tentukan dan *button* oke di klik, maka akan di minta untuk *login* kembali untuk mendapatkan kode OTP yang baru.

3. *Black box id user*

Black box id user berguna untuk mengetahui *delay* atau jedak waktu pengiriman kode otp ke aplikasi android setelah *user* berhasil melakukan *login* (lihat tabel 4).

Tabel 4. *Black Box Id User*

ID	**Percobaan**	**Hasil uji yang di harapkan**	***Delay***	**Hasil**
664802529	1	Kode terkirim	9 detik	✓
	2	Kode terkirim	7 detik	✓
	3	Kode terkirim	5 detik	✓
	4	Kode terkirim	8 detik	✓
	5	Kode terkirim	10 detik	✓

Keterangan :

Pengujian pengiriman Kode OTP ke *user* melalui aplikasi android memiliki *delay* atau jeda waktu berkisar 5 detik sampai 10 detik.

Pengujian pengiriman Kode OTP ke user memiliki selisih waktu 1 detik sampai 5 detik.

Hasil Ahli Media dan Ahli Materi

Hasil uji ahli media berguna untuk mengetahui kelayakan dari ahli media yang melibatkan ahli media yang berpengalaman dibagiannya. Hasil uji ini dilakukan dengan 3

aspek data validasi yang di dapat berupa tampilan media, kegunaan, dan bahasa pemograman. Persentase kelayakan yang di dapat adalah 82% dan dapat disimpulkan sangat layak, seperti yang terlihat pada tabel 5. Sementara itu, hasil uji ahli materi berguna untuk mengetahui kelayakan dari ahli materi yang melibatkan ahli media yang berpengalaman dibagiannya. Hasil uji ini dilakukan dengan 3 aspek data validasi yang di dapat berupa desain, isi, dan pembelajaran. Persentase kelayakan yang di dapat adalah 75% dan dapat disimpulkan layak, seperti yang terlihat pada tabel 6.

Tabel 5. Persentase Ahli Media

No	Aspek	Persentase	Kategori
1.	Tampilan Media	80%	Sangat Layak
2.	Kegunaan	85%	Sangat Layak
3.	Bahasa Pemograman	80%	Sangat Layak
	Rata – Rata	**82%**	**Sangat Layak**

Tabel 6. Persentase Ahli Materi

No	Aspek	Persentase	Kategori
1.	Desain	75%	Layak
2.	Isi	78%	Layak
3.	Pembelajaran	72%	Layak
	Rata – Rata	**75%**	**Layak**

Pembahasan

Berdasakan dari hasil di atas, pengimplementasi *One Time Password* (OTP) pada sitem *login* di aplikasi penagihan hutang berbasis web berjalan sangat baik dengan menggunakan bahasa pemograman PHP. Dalam pengembangan sistem ini peneliti menerapkan metode *Waterfall Development* di mana memiliki tahapan – tahapan, diantaranya ; *Planning, Analysis, Design, Implemenstation*, dan *Testing*. Tahap – tahap ini berguna untuk menentukan apa saja yang di butuhkan dalam mengembangkan sistem dengan cara observasi langsung ke perusahaan. *One Time Password* sistem keamanan login untuk *account user* di aplikasi ini, berhasil terkirim melalui aplikasi android dan dapat digunakan satu kali saat *user* tersebut melakukan login. Namun proses penginputan juga mempunyai batas waktu yang berguna sebagai validasi oleh yang dilakukan oleh sistem. Kelayakan sistem keamanan *account* diuji menggunakan *blackbox* dan validasi yang melibatkan beberapa pihak. Pihak yang terlibat dalam pengujian ini adalah ahli media dan ahli materi.

Validasi ahli media terdiri dari tiga aspek, yaitu: Tampilan Media, Kegunaan dan Bahasa Pemograman. Berdasarkan hasil penilaian pada aspek tampilan media pengembangan keamanan login berbasis web dengan pernyataan kesesuaian tata letak dan penggunaan jenis *font*, kejelasan warna teks dan *button* dengan background didapatkan skor persentase sebesar 80% dengan kategori Sangat Layak. Sedangkan aspek kegunaan dengan pernyataan kemudahan pengoperasian aplikasi, kejelasan dalam menggunakan aplikasi mendapatkan skor persentase sebesar 85% dan dikategorikan Sangat Layak. Sedangkan aspek bahasa pemograman dengan penamaan variabel, *function* dan alur proses algoritma SHA-512 mendapatkan skor persentase sebesar 80% dan dikategorikan Sangat Layak. Dari hasil persentase ketiga aspek itu di dapat sebuah nilai rerata persentase sebesar 82%. Angka ini dapat di nyatakan dalam kategori Sangat Layak jika diambil berdasarkan dari tabel 1. Namun seiring kebutuhan perusahaan aplikasi ini dapat terus di kembangkan walaupun hasil yang di dapat sangat memuaskan dalam pengembangan *One Time Password* (OTP) pada aplikasi ini.

Saran dan masukan dari ahli media sangat di butuhkan dalam melakukan perbaikan dalam pengembangan.

Validasi ahli materi terdiri dari tiga aspek, yaitu ; Desain, Isi dan Pembelajaran. Berdasarkan hasil penilaian terhadap aspek desain isi dengan pernyatan kejelasan tujuan, isi, dan penggunaan aplikasi didapatkan skor persentase sebesar 75% dengan kategori Layak. Pada aspek isi dengan pernyataan kualitas isi, cakupan isi, serta kedalaman isi didapatkan skor persentase sebesar 78% dengan kategori Layak. Sedangkan aspek pembelajaran penyampaian modul, kemudahan memahami modul dalam proses pengerjaan dengan mendapatkan skor persentase sebesar 72% dan dikategorikan Layak. Dari hasil persentase ketiga aspek itu di dapat sebuah nilai rerata persentase sebesar 75%. Angka ini dapat di nyatakan dalam kategori Layak jika di dambil berdasarkan dari tabel 1. Namun seiring kebutuhan perusahaan aplikasi ini dapat terus di kembangkan walaupun hasil yang di dapat sangat memuaskan dalam pengembangan *One Time Password* (OTP) pada aplikasi ini. Saran dan masukan dari ahli materi sangat di butuhkan dalam melakukan perbaikan dalam pengembangan.

Berdasarkan penilaian validasi oleh ahli media ahli materi dan dapat di ambil garis besar bahwa pengembangan *One Time Password* (OTP) aplikasi ini layak di gunakan. Keamanan *account user* dapat terjaga dengan baik karena kode angka hanya dapat di gunakan sekali saat *user* melakukan *login* dan sistem dapat meng – otentikasi bahwa yang menggunakan kode angka tersebut benar – benar user itu sendiri. Otentikasi dapat menghindari dari penyalahan gunaan *account* dari orang yang tidak berkepentingan.

SIMPULAN

Berdasarkan penelitian dan pembahasan, implementasi *One Time Password* (OTP) menggunakan Algoritma SHA-512 pada aplikasi penagihan hutang PT. XHT ini menggunakan metode *Waterfall Development*. Hasil uji dari *blackbox* menunjukkan bahwa pengembangan sistem keamanan *login* ini berfungsi dengan baik dan sesuai dengan hasil yang di harapkan.Hasil kelayakan media dari ahli media mendapat total persentase sebesar 82% dengan kategori sangat layak dan hasil kelayakan materi dari ahli materi mendapat total persentase sebesar 75% dengan kategori layak.

REFERENSI

Adilah, S., Mangkudjaja, R. R., & Paryasto, M. W. (2017). Implementasi Kriptosystem menggunakan metode Algoritma ECC dengan Fungsi Hash SHA-256 pada sistem ticketing online Implementation of Crypthosystem using Method Algorithm ECC with Function of Hash SHA- 256 in online ticketing system. *E-Proceeding of Engineering* (pp.4138–4146). Indonesia: Telkom University press.

Al Azam, M. N. (2016). Otentikasi Sistem Dengan Menggunakan One Time Password Memanfaatkan Smartphone Android. *Link*, *24*(1), 7–10.

Dewy, N. A. (2018). Kontrol Akses Pintu Rumah Menerapkan Konsep OTP (One Time Password) Untuk Meningkatkan Keamanan Dengan Implementasi IoT (Internet Of Things). *JATI (Jurnal Mahasiswa Teknik Informatika)*, *2*(1), 467–473.

Khairina, D. M. (2011). Analisis Keamanan Sistem Login. *Jurnal Informatika Mulawarman*, *6*(2), 64–67.

Kinarwanto, B. (2016). Faktor-Faktor Pemanfaatan Teknologi Informasi dan Pengaruhnya Terhadap Kinerja Individual (Studi pada PDAM Kota Malang). *Jurnal Ilmiah Mahasiswa Fakultas Ekonomi Dan Bisnis*, *1*(2), 1–19.

Kurniawan, M. B., & Fatimah, T. (2018). Aplikasi Nilai Online Menggunakan One Time Password Dengan Algoritma Sha 512 Berbasis Web Pada Smp Pgri 336. *Skanika*, *1*(1), 411–416.

Mulya, M. (2009). Penggunaan Algoritma SHA-512 Untuk Menjamin Integritas dan Keotentikan Pesan Pada Intrainet. *Konferensi Nasional Sistem Dan Informatika* (pp.107–111). Indonesia: STMIK STIKOM Bali press

Naufal, M., & Purwanto. (2018). Implementasi Keamanan Login Dengan Metode One Time Password (Otp) Menggunakan Fungsi Hash Algoritma Sha-512. *Skanika*, *1*(1), 335–339.

Pressman, R. (2003). *Rekayasa Perangkat Lunak Pendekatan Praktis.* 2nd, Andi. Yogyakarta. Indonesia.

Sakti, D. V. S. Y., Agani, N., & Hardjianto, M. (2016). Pengamanan Sistem Menggunakan One Time Password Dengan Pembangkit Password Hash SHA-256 dan Pseudo Random Number Generator (PRNG) Linear Congruential Generator (LCG) di Perangkat Berbasis Android. *Budi Luhur Information Technology*, *13*(1), 1–10.

Saptohadi, W., Ritzkal, & Prakosa, B. A. (2018). Implementasi QR Ccode Dinamic Pada Sistem One-Time Password (OTP) Sebagai Key Penggerak Solenoid Berbantuan Arduino Mega 2560. *Seminar Nasional Teknologi Informasi* (pp.782–788). Indonesia: Universitas Ibn Khaldun press

Sugiyatno, & Atika, P. D. (2018). Digital Signature Dengan Algoritma Sha-1 Dan Rsa Sebagai Autentikasi. *Jurnal Cendikia*, *16*(2), 74–83.

Wadhwani, S., Singh, U., Singh, P., & Dwivedi, S. (2018). Smart Home Automation and Security System using Arduino and IOT. *International Research Journal of Engineering and Technology (IRJET)*, *5*(2), 1357–1359.

Wijaya, C. H., Hendrawan, A. H., Pramuko, A. E. K., & Goeritno, A. (2017). Implementasi Sistem One-Time Password (OTP) Sebagai Key Penggerak Kunci Pintu berbantuan Arduino Uno. *Seminar Nasional Inovasi Dan Aplikasi Teknologi Di Industri* (pp.1–7). Indonesia: ITN Malang press.

Yahya, N. I., & Amini, S. (2018). Pengimplementasia One Time Password dan Notifikasi Email menggunakan Fungsi Hash SHA-512 Berbasis Web Pada SMK Cyber Media. *Skanika*, *1*(2), 745–750.