CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 3, No. 2, November 2020, hlm. 6-11

ONE-TIME-PASSWORD (OTP) DENGAN MODIFIKASI *VIGENERE CHIPER* DAN PERANGKAT USB BERBASIS *MICROCONTROLLER*, SENSOR *FINGERPRINT*, DAN *REAL TIME CLOCK* (RTC) UNTUK AUTENTIKASI PENGGUNA PADA AKSES APLIKASI WEB

Muhammad Anis Al Hilmi[1], A Sumarudin[2] , Willy Permana Putra[2]

[1,2,3]Politeknik Negeri Indramayu
Email: [1]alhilmi@polindra.ac.id, [2]shumaru@polindra.ac.id, [3]willy_p@polindra.ac.id

(Naskah masuk: 09 Agustus 2020, diterima untuk diterbitkan: 31 November 2020)

Abstrak

Hampir semua aplikasi *web* yang memerlukan pengesahan / autentikasi, menggunakan mekanisme verifikasi *password* untuk masuk ke dalam sistem. Bagi pengguna, *password* adalah dilema. *Password* yang aman seringkali sulit untuk diingat, sedangkan *password* yang mudah diingat biasanya mudah untuk ditebak. Pengguna juga melakukan hal teledor seperti menulis *password* di *sticky note* dan semacamnya, juga menggunakan *password* yang sama untuk akun berbeda sehingga membuat keamanan akun semakin rentan, terutama karena serangan dengan *keylogger*. Untuk mengatasi hal ini, telah dikembangkan beberapa teknik pengamanan, seperti menambah faktor lain ketika *login* dengan kode *One-Time-Password* (OTP) lewat SMS, perangkat *token generator* seperti yang dipakai perbankan, *login* dengan *hardware* USB, akses lewat *sensor* biometrik *fingerprint*, bahkan *electrocardiogram* (ECG). Dengan menilik kelebihan dan kekurangan aneka pendekatan yang telah dikembangkan serta dengan orientasi fokus kepada kemudahanan pengguna, penelitian ini mengusulkan perangkat dan metode untuk memperkuat keamanan sistem dalam proses *login*, dan tetap mudah dalam penggunaannya (tanpa secara manual mengingat, memasukkan *username* dan *password*), portabel, dan terjangkau. Pada makalah ini autentikasi dengan OTP diajukan dengan metode Vigenere Chiper yang dimodifikasi dengan nilai *salt* yang selalu berubah dan pengacakan data menggunakan algoritma *butterfly*. Ditambah pengamanan menggunakan perangkat keras berbasis *microcontroller*, sensor *fingerprint*, dan modul *Real-Time-Clock* (RTC) untuk validasi kepemilikan dan sinkronisasi waktu dalam mencegah *keylogger attack*. Hasil pengujian memperlihatkan perangkat dapat menghasilkan OTP dengan waktu rata-rata 0,956 sekon, dan memudahkan pengguna untuk *login* ke aplikasi web tanpa perlu mengingat *password*.

Kata kunci: *Autentikasi, Kriptografi, OTP, Vignere Chiper, Microcontroller, Fingerprint*

ONE-TIME-PASSWORD (OTP) USING MODIFICATION OF VIGENERE CHIPER AND USB DEVICES BASED ON MICROCONTROLLER, FINGERPRINT SENSOR, AND REAL TIME CLOCK (RTC) FOR USER AUTHENTICATION ON WEB APPLICATION ACCESS

Abstract

Most web applications that require authentication / authentication use a password verification mechanism to log into the system. For users, passwords are a dilemma. Secure passwords are often difficult to remember, while passwords that are easy to remember are usually easy to guess. Users also do careless things such as writing passwords on sticky notes and the like, also using the same password for different accounts, making account security even more vulnerable, especially due to attacks with keyloggers. To overcome this, several security techniques have been developed, such as adding other factors when logging in with a One-Time-Password (OTP) code via SMS, token generator devices such as those used by banks, logging in with USB hardware, access via biometric fingerprint sensors, even electrocardiogram (ECG). By looking at the advantages and disadvantages of various approaches that have been developed and with a focus on user convenience, this study proposes tools and methods to strengthen system security in the login process, and remain easy to use (without manually remembering, entering username and password), portable. , and affordable. In this paper, OTP authentication is proposed using the modified Vigenere cipher method with a constantly changing salt value and data randomization using the butterfly algorithm. Plus security uses microcontroller-based hardware,

fingerprint sensors, and Real-Time-Clock (RTC) modules for validation of ownership and time synchronization to prevent keylogger attacks. The test results show the device can generate OTP with an average time of 0.956 seconds, and makes it easier for users to log into web applications without needing to remember password.

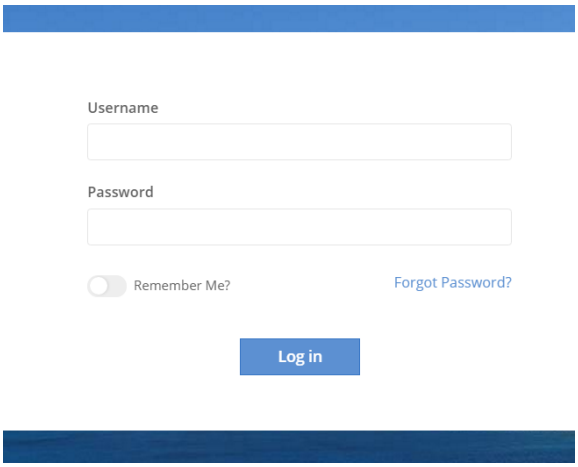
Keywords: *Authentication, Cryptography, OTP, Vigenere chiper, Microcontroller, Fingerprint*

1. PENDAHULUAN

Dalam keseharian, kita menjumpai mekanisme autentikasi untuk dapat mengkases sesuatu. Misalkan, dalam penggunaan mesin ATM (Anjungan Tunai Mandiri), kita diminta memasukkan nomor PIN. Untuk bisa mengakses akun sosial media, Instagram misalnya, kita juga diminta memasukkan alamat email atau *username* dan *password*. Ketika akan berbelanja di toko online ataupun *e-commerce*, untuk melakukan transaksi, kita diminta memasukkan *username*, *password*, dan tidak jarang juga ditambah kode OTP (*One Time Password*) sebagai unsur validasi tambahan. Terdapat beberapa pengembangan sistem keamanan, misalnya login ditambah dengan faktor lain seperti kode OTP (*One Time Password*) lewat SMS (Santoso, 2013), perangkat *token generator* seperti yang dipakai perbankan (Syarif, 2018), *login* dengan *hardware USB* (Künnemann, 2012), (Yu, 2010), akses lewat *sensor* biometrik *fingerprint*, bahkan *electrocardiogram* (ECG) (Arteaga-Falconi, 2018).

Di tengah kondisi *cyber security* terkini, tentu sebaiknya setiap akun memiliki *username* dan *password* yang berbeda. Semakin banyak akun yang dimiliki, tentu banyak pula data *username* dan *password* yang perlu dikelola dan dihafal. Bagi pengguna, *password* adalah dilema. *Password* yang aman seringkali sulit untuk diingat, sedangkan password yang mudah diingat biasanya mudah untuk ditebak. Pengguna juga melakukan hal teledor seperti menulis *password* di *sticky note* dan semacamnya (Sharevski, 2019) yang mana akan membuat keamanan akun semakin rentan.

Hampir semua aplikasi *web* dan *mobile* mengadopsi sistem autentikasi seperti tersebut di atas. Bukan tanpa alasan, mekanisme tersebut sudah menjadi kewajiban, terutama untuk mengakses sistem yang memuat data penting dan privat, misalnya data diri, transaksi perbankan, dan rekam medis. Hal ini mengingat semakin banyaknya jumlah serangan *cyber* dan usaha pencurian data/penipuan yang memanfaatkan fakta bahwa penggunaan internet semakin meluas, adanya celah di aplikasi, dan keteledoran pengguna.



Gambar 1. Contoh Tampilan Login

Kaspersky Lab dalam laporannya selama kuartal II (Q2) tahun 2019, menyebutkan bahwa terdapat 8.275.318 ancaman siber *internet-borne* yang berbeda pada komputer para pengguna Kaspersky Security Network (KSN) di Indonesia. Secara keseluruhan, 28,5% pengguna diserang oleh ancaman yang ditularkan melalui *web* (Redaksi WE Online, 2019). Hal ini tentu berkaitan dengan akses internet yang meluas dan meningkat di Indonesia. Survei APJII pada tahun 2018 tentang penetrasi dan profil perilaku pengguna internet Indonesia, menyatakan bahwa 171,17 juta jiwa penduduk Indonesia adalah pengguna internet aktif, dengan kata lain 64,8% dari seluruh jumlah penduduk. Dengan persentase pertumbuhan pengguna 10,12% per tahun (APJII, 2018).

Gambar 2. Infografis Penetrasi Pengguna Internet (APJII, 2018)

Dari yang telah dijabarkan di atas, serta dengan orientasi fokus kepada pengguna, dalam penelitian ini diusulkan mekanisme dan perangkat/*device* tambahan untuk memperkuat *password* dan proses *login* ke dalam suatu sistem aplikasi *web* ataupun *mobile*, yang mudah digunakan (tanpa secara manual

memasukkan *username* dan *password*), mudah dibawa, dan terjangkau.

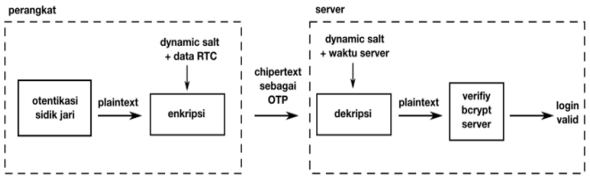
Di pasaran, terdapat produk dari Yubico (Yubico, 2010), yaitu perangkat USB untuk men-*generate* OTP seperti gambar berikut.

Gambar 3. Produk Yubico

Perangkat tersebut akan menghasilkan OTP jika dipasang ke konektor USB komputer, *laptop*, dan *smartphone*, di-*trigger* dengan menyentuhkan jari di permukaan tengahnya. Namun perangkat di atas memiliki kelemahan, yaitu siapa saja dapat menggunakan, walaupun bukan pemilik aslinya, karena yang dibutuhkan hanya listrik statis dari jari tangan manusia. Hal ini tentu menjadi riskan.

2. METODE

2.1. Blok Diagram Sistem



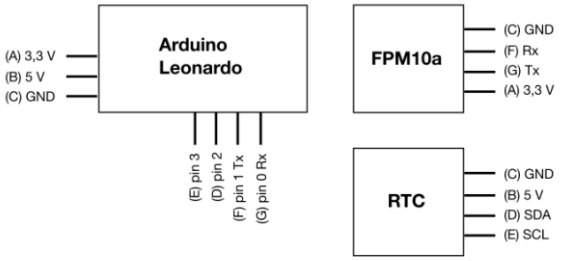
Gambar 4. Blok Diagram

Dalam penelitian ini, diajukan 2 sistem pengamanan *password*, yaitu dengan perangkat keras dan aplikasi *web*.

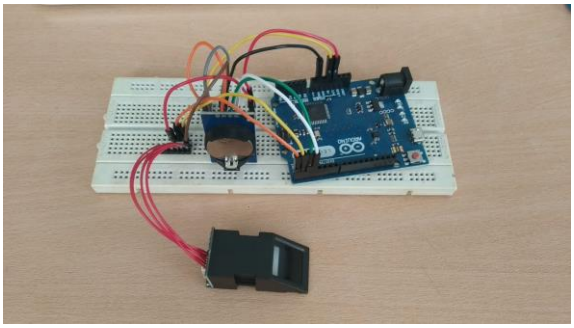
Mengacu pada Gambar 4, yaitu blok diagram dari sistem keseluruhan. Ketika pengguna memasang perangkat ke *laptop* atau komputer, kemudian ketika pengguna menempelkan jari di *sensor* sidik jari, identitas pengguna akan diperiksa dan diautentikasi. Setelah itu, perangkat akan melakukan enkripsi dengan algoritma khusus dan pengacakan dengan metode *butterfly* atas data berupa plaintext ditambah dengan angka acak, *dynamic salt*, dan data dari modul RTC. Hasil dari enkripsi, *chipertext* digunakan sebagai sandi *one-time-password*, OTP, untuk input data suatu laman web dengan terlebih dahulu diproses. Data *chipertext* didekripsi dengan angka acak, *dynamic salt* dari *chipertext* dan waktu, *timestamp* yang berjalan di sisi *server*. Setelah itu data diperbaiki urutannya dengan metode *reverse-butterfly* dan dihasilkan *plaintext*. Setelah itu, di tahap terakhir *server* melakukan verifikasi algoritma Bcrypt dari basis data di sisi server, jika lolos semua tahap, pengguna dapat masuk atau *login* ke dalam laman *web* tertentu.

2.2. Perangkat keras

Perangkat keras terdiri dari *sensor* sidik jari, modul *real-time-clock* (RTC), dan Arduino Leonardo. Sensor sidik jari yang dipakai adalah seri FPM10a, menggunakan antarmuka UART dan dapat menyimpan hingga 1000 data. Modul RTC yang digunakan adalah DS3231 dengan *power* berupa baterai CR2032 untuk dapat beroperasi. Sedangkan *board* yang digunakan adalah Arduino Leonardo, yang mana mempunyai kemampuan USB HID, artinya dapat menjadi *High Interface Device* (HID) untuk berkomunikasi dengan komputer, sebagai perangkat inputan berupa *mouse* atau *keyboard*. Berikut skema rangkaiannya.



Gambar 5. Skema rangkaian

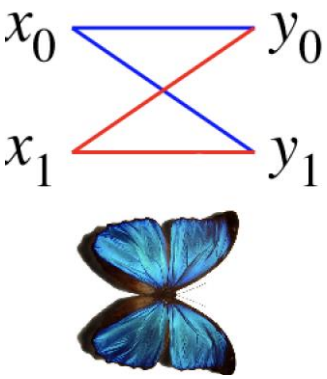


Gambar 6. Prototype

Pseudocode Enkripsi

```
DP = n Data perangkat;
TS = get Timestamp dari RTC;
// Key = secret key
// generate n digit random salt
for (byte i = 0; i < n; i = i + 1)
{
       Salt[i] = random();
}
//Chipertext = Encrypt (DP + TS, Salt)
for (byte i = 0; i < n; i = i + 1)
{
// ([DP, TS -> Data] + salt) mod Key
       ChiperText[i]   =   (Data[i]   +
       Salt[i]) % Key;
```

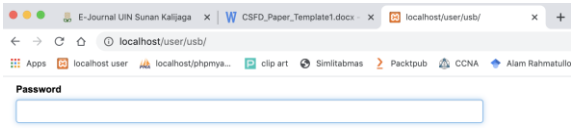
```
}
/* Acak index data, metode radix / butterfly */
Output = butterfly()
// Autentikasi sidik jari
if(finger.fingerID == valid)
//sidik jari dikenali?
{
      /* keluarkan output data dalam bentuk teks */
      for (byte i = 0; i < 32; i = i + 1) {
      //32 char output
      Keyboard.print(outputButterfly[i]);
}
      Keyboard.println();

}
```



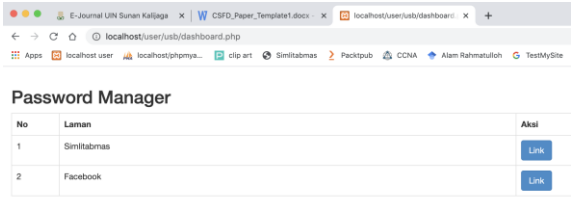
Gambar 7. Pengacakan data silang

2.3. Aplikasi Web

Pada aplikasi web, sebagai *proof-of-concept* (PoC) dibuat menjadi 2 halaman, yaitu *login* dan *dashboard* ketika *login* berhasil.



Gambar 8. Tampilan *login*



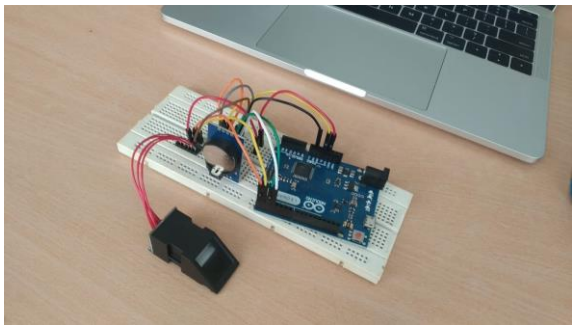
Gambar 9. Tampilan *dashboard*

Pseudocode Dekripsi

```
Get 32 char data;
Get server Timestamp;
// Normalisasi index data
Reverse-butterfly();
Get data perangkat;
Get Timestamp perangkat;
/* Periksa data perangkat di database server */
if(data perangkat == valid) /*data ada di db? */
{
      /* Periksa timestamp apakah sinkron? */
      Compare (timestamp perangkat, timestamp server);
      if(sinkron == valid)
      {
            login;
      }
      else
      gagal login karena data kadaluarsa;
}
else
      gagal login karena user tidak valid;
```

3. Hasil dan Pembahasan

Dari hasil implementasi, berupa perangkat keras dan aplikasi web, kemudian dilakukan pengujian atas hasil keluaran teks OTP dan berapa lama kebutuhan waktunya.



Gambar 10. PoC perangkat keras

```
14:33:17.944 -> mulai
14:33:18.939 -> 845889479682351504090924690905 85
```

Gambar 11. Data hasil dan konsumsi waktu

Tabel 1. Hasil teks keluaran dan konsumsi waktu

No	Data	Durasi Proses (mS)
1	233791202151532851761645266621O5	863
2	00167020205072485277379527679275	988
3	364206509626986895103095701085O5	932
4	79850950295991686186369576169175	848
5	74805400346486582742521562021795	982
6	10268030801042183358086548886345	990
7	28341860982870486388389548888365	890
8	85915500558537081934440534746945	1001
9	51677120912153284863531513534825	1010
10	88942870588860383459692529697455	1002
11	14207420144476487499894589297455	1013
12	98045800588820981237874557979275	994
13	06125600467638087297874587270285	894
14	213771202151532851761675266621O5	972
15	05116510851507781631016571119675	994
16	25314590558597688601319591310685	951
17	36428630366608786489490509494425	924
18	63794390336305784762026582229775	939
19	53697320235365387095551595355035	962
20	49555900598921988207470557971295	970
	Rata-rata	955,95

4. Penutup

Pada penelitian ini *proof-of-concept* (PoC) autentikasi dengan OTP diajukan dengan metode Vigenere Chiper yang dimodifikasi dengan nilai *salt* yang selalu berubah dan pengacakan data menggunakan algoritma *butterfly*. Ditambah pengamanan menggunakan perangkat keras berbasis *microcontroller*, *sensor fingerprint*, dan modul *Real-Time-Clock* (RTC) untuk validasi kepemilikan dan sinkronisasi waktu dalam mencegah *keylogger attack*. Hasil pengujian memperlihatkan perangkat dapat menghasilkan OTP dengan waktu rata-rata 0,956 sekon, dan memudahkan pengguna untuk *login* ke aplikasi web tanpa perlu mengingat *password*. Ke depannya dapat dikembangkan ke arah integrasi *browser* dan penguatan di sisi enkripsi, juga penambahan karakter selain angka, misalkan huruf dan simbol.

Ucapan Terima Kasih

Penelitian ini didanai oleh DIPA Polindra pada skema Penelitian Dosen Pemula (PDP) Internal Tahun 2020.

DAFTAR PUSTAKA

APJII. 2018. Penetrasi & Profil Perilaku Pengguna Internet Indonesia.

ARTEAGA-FALCONI, J. S., Al Osman, H., & El Saddik, A. 2018. ECG and fingerprint bimodal authentication. *Sustainable cities and society*, *40*, 274-283.

GOOGLE DEVELOPER. 2016. Access USB Devices on the Web. https://developers.google.com/web/updates/2016/03/access-usb-devices-on-the-web. Diakses pada 7 Januari 2020.

HAJIAN, M. 2019. Modern Web APIs. In *Progressive Web Apps with Angular* (pp. 289-330). Apress, Berkeley, CA.

JAIN, A. K., Ross, A., & Prabhakar, S. 2004. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, *14*(1).

JAIN, A. K., P. Flynn, and A. A. Ross, Eds. 2007. Handbook of Biometrics. New York: Springer.

KELLEY, DIANA. 2019. Microsoft Security Intelligence Report Volume 24. https://www.microsoft.com/security/blog/2019/02/28/microsoft-security-intelligence-report-volume-24-is-now-available/. Diakses pada 6 Januari 2020.

KÜNNEMANN, R., & STEEL, G. 2012. YubiSecure? Formal security analysis results for the Yubikey and YubiHSM. In *International Workshop on Security and Trust Management* (pp. 257-272). Springer, Berlin, Heidelberg.

OBDEV. V-USB. https://www.obdev.at/products/vusb/index.html. Diakses pada 7 Januari 2020.

ORACLE. 2010. Specifying Authentication Mechanisms. https://docs.oracle.com/cd/E19798-01/821-1841/gkbsa/index.html. Diakses pada 6 Januari 2020.

PIHLAJAMAA, JOONAS. 2012. DIY USB password generator. https://codeandlife.com/2012/03/03/diy-usb-password-generator/. Diakses pada 7 Januari 2020.

REDAKSI WE ONLINE. 2019. Kondisi Keamanan Siber Indonesia selama Kuartal II 2019, Amankah? https://www.wartaekonomi.co.id/read236815/kondisi-keamanan-siber-indonesia-selama-kuartal-ii-2019-amankah.html. Diakses pada 7 Januari 2020.

SANTOSO, K. I. 2013. Dua Faktor Pengamanan Login Web Menggunakan Otentikasi One Time Password Dengan Hash SHA. *Semantik*, *3*(1).

SHAREVSKI, F., TREEBRIDGE, P., & WESTBROOK, J. 2019. *Experiential User-Centered Security in a Classroom: Secure Design for IoT. IEEE Communications Magazine, 57(11), 48–53*. doi:10.1109/mcom.001.1900223

SUHENDRA, A., YULIANTI, A., JUNATAS, B., & VALENTINE, V. 2008. Modified Authentication using One Time Password to SupportWeb Services Security. In *WOSOC 2008-Workshop on Open Source and Open Content, 1-3 December 2008*. Bali.

SUO, X., Y. ZHU, AND G. OWEN. 2005. Graphical passwords: A survey,‖ in Proc. Annu. Computer Security Applications, pp. 463– 472

SYARIF, A. F., BASUKI, P. N., & WIJAYA, A. F. 2018. Analisis Kinerja Sistem Informasi pada PT. Bank Central Asia Menggunakan IT Balanced Scorecard. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, *7*(1), 1-6.

WANG, C., JAN, S. T., HU, H., BOSSART, D., & WANG, G. 2018. The next domino to fall: Empirical analysis of user passwords across online services. In Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (pp. 196-203). ACM.

YU, J., & ZHANG, C. 2010. Design and Analysis of a USB-Key Based Strong Password Authentication Scheme. 2010 International Conference on Computational Intelligence and Software Engineering. doi:10.1109/cise.2010.5676914

YUBICO, A. B. 2010. Kungsgatan 37, 111 56 Stockholm Sweden. The YubiKey Manual-Usage, configuration and introduction of basic concepts (Version 2.2).

ZOHO. What is password management? https://www.zoho.com/vault/educational-content/what-is-password-management.html. Diakses pada 7 Januari 2020.