Available online to ejournal.pnc.ac.id

Journal of Innovation Information Technology and Application

Journal Page is available to https://ejournal.pnc.ac.id/index.php/jinita

Pengembangan Metode *Login Two Factor Authentication* (2FA) untuk Keamanan Sistem Informasi Akademik

Yusuf Heriyanto [1], Anas Azhimi Qalban [2)], Iif Alfiatul Mukaromah [3]*

[1,2,3] Fakultas Dakwah, UIN Saizu Purwokerto, Indonesia*

email:[1] yusuf@uinsaizu.ac.id, [2] anasaq@uinsaizu.ac.id, [3] iifam@uinsaizu.ac.id*

ARTICLE INFO

Article history:
Received 17 November 2022
Revised 30 November 2022
Accepted 19 December 2022
Available online 30 December 2022

Keywords:
Two-factor authentication
Sistem informasi

IEEE style in citing this article:
Y. Heriyanto, A. A. Qalban, and I. A. Mukaromah, "Pengembangan Metode Login Two Factor Authentication (2FA) untuk Keamanan Sistem Informasi Akademik," Journal of Innovation Information Technology and Application (JINITA), vol. 4, no. 2, pp. 142–150, Dec. 2022..

ABSTRACT

Massive transformation in the era of society 5.0 brings many changes to the lifestyle of mankind, one of which is in the educational aspect. Educational organizations are competing to improve the quality of education, especially in the quality of academic services. The transition from a conventional academic service model to an academic information system model has made new changes in educational organizations. Security issues arise when implementing an academic information system caused by several factors including the user's negligence in securing login passwords, thus the motivation of this paper is how to overcome these weaknesses. This study proposes a two-factor authentication (2FA) verification method that collaborated with the Telegram application in order to help minimize weaknesses in the security of academic information systems. The results of this study are able to provide access security both from the user's and the user's side since the 2FA method applies the OTP strategy and calculation authentication in addition to the password method to access academic information systems. This method was the initial idea for securing an academic information system, therefore irresponsible people could not easily log into it.

1. PENDAHULUAN

Era digital yang saat ini disebut dengan era *society* 5.0 merupakan upaya umat manusia untuk melakukan aktifitas apapun secara mudah secara *online* [1]. Perkembangan era digital memberikan perubahan signifikan terhadap dunia pendidikan dimana semakin meningkatnya kualitas pelayanan dan pembelajaran sehingga semakin mengurangi kelemahan metode pelayanan dan pembelajaran tradisional [2]. Transformasi layanan yang begitu marak ke ranah *online* oleh pengguna internet telah meningkatkan kebutuhan akan autentikasi yang lebih baik. Pengguna sekarang perlu mengelola kemampuan mereka dalam mengelola dan mengingat sandi yang digunakan. Perangkat lunak *browser* khusus yang memiliki kemampuan pengelola kata sandi dapat menjadi solusi, tetapi juga para peneliti telah menyimpulkan bahwa pengelola kata sandi dapat memperburuk situasi dalam kasus tertentu [3]. Era sekarang sudah umum bagi pengguna untuk menggunakan kemampuan pengelolaan sandi yang disediakan oleh *browser* sehingga dapat menimbulkan konsekuensi serius jika aplikasi tersebut tidak berada pada *device* pribadi pengguna. Metode keamanan *two-factor authentication* (2FA) diusulkan untuk mengatasi isu penanggulangan sisi *server* untuk mencegah pencurian kata sandi [4].

Sistem informasi akademik sebagai media pelayanan dan pembelajaran pada dunia pendidikan terkini membutuhkan sebuah terobosan baru kaitannya terhadap keamanan sistem [5]. Hal ini dapat kita ketahui bahwa tumpukan *big data* yang terdapat pada sistem informasi akademik merupakan data yang bersifat pribadi atau rahasia, sehingga celah-celah keamanan yang menjadi gerbang terbukanya peluang

**) Penulis Korespondensi : anasaq@uinsaizu.ac.id*

kejahatan *cyber* haruslah melakukan antisipasi sedini-dininya [6]. Pengembang sistem telah melakukan upaya terus-menerus untuk memberikan sistem keamanan yang baik, desain *two-factor authentication* yang aman dan efisien masih menjadi pertanyaan terbuka apakah dapat menjawab tantangan yang terjadi [7]. Sistem keamanan dengan mengembangkan metode 2FA menggunakan kode *one time password* (OTP) via aplikasi Telegram dan autentikasi kalkulasi sebagai pencegahan awal terhadap serangan *cyber*. Cara ini merupakan model perlindungan keamanan berlapis yang dapat meminimalisir akses orang yang tidak memiliki wewenang terhadap akun pengguna sehingga mempersulit langkah pelaku kejahatan *cyber* untuk masuk ke dalam sistem informasi dan tentunya memberikan keuntungan bagi pengguna dan pengembang sistem agar data privasi tidak mudah diakses orang yang tidak berwenang[8].

Penelitian sebelumnnya telah mengungkapan bagaimana pemanfaatan metode 2FA terhadap sistem informasi mereka. Model yang pertama adalah *physically uncloneable functions* (PUFs) yang digunakan untuk ketahanan dan efisiensi sistem terhadap serangan *cyber* [8]. Model berikutnya penggabungan *physically uncloneable functions* (PUFs) dan *voiceprint* yang disebut dengan metode *transparent two-factor authentication* (T2FA) untuk memberikan pengguna kenyamanan serta rasa aman saat berinteraksi diranah digital [9]. Penelitian berikutnya adalah pengembangan model keamanan dengan mengembangkan *sound-proof* yang dapat dengan mudah digunakan melalui *smartphone* dan *browser* utama tanpa *plugin* [10]. Masih banyak lagi penelitian yang berkaitan dengan 2FA untuk meningkatkan keamanan penggunaan sistem informasi. Penelitian ini mengusulkan pemanfaatan metode 2FA sebagai solusi tantangan terhadap keamanan sistem informasi akademik.

Aplikasi pengirim pesan instan Telegram dipilih dalam implementasi Metode 2FA ini, karena aplikasi pesan instan Telegram merupakan aplikasi pengirim pesan instan yang cukup popular dan banyak digunakan oleh masyarakat *modern* [11]. Telegram memiliki kemampuan memberikan otomasi pesan dengan menyediakan fasilitas bot *Application Programming Interface (API)* yang dilengkapi kemampuan dokumentasi dan fitur yang lengkap dan gratis [12]. Pemanfaatan teknologi berbasis bot dinilai dapat memberikan jaminan autentikasi yang lebih baik untuk mengidentifikasi pengguna.

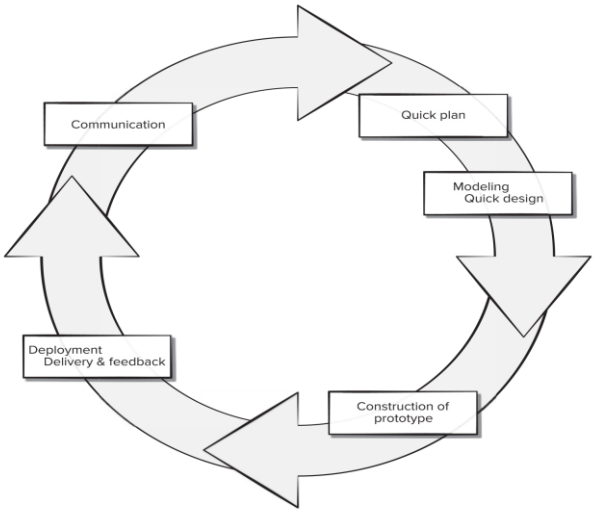
Metode 2FA diusulkan sebagai jawaban dari isu keamanan sistem, penelitian ini berfokus pada pengamanan sistem informasi akademik pada bagian awal penggunaan sistem yang diharapkan dapat mengantisipasi langkah lanjutan kejahatan *cyber* jika sudah bisa masuk ke dalam *dashboard* pengguna. Berkolaborasi dengan model *one time password* (OTP) melalui aplikasi Telegram dan model autentikasi kalkulasi, maka keamanan sistem informasi akademik diharapkan akan lebih baik dan dapat memberikan kenyamanan kepada pengguna kaitan dengan kewajiban pengembang untuk menjaga sandi dan akun pengguna.

2. METODE PENELITIAN

Penelitian ini melakukan analisa dengan pendekatan prespektif model *prototyping* dengan pengembangan metode *two-factor authentication* (2FA) [13]. Analisa dilakukan dengan merujuk pada isu yang ditemukan pada saat implementasi sistem informasi akademik. Peneliti melihat adanya indikasi budaya *user* yang lebih suka menyimpan passwordnya pada *browser*, sehingga rentan jika hal tersebut dilakukan di komputer umum seperti di komputer orang lain, laboratorium atau layanan akademik umum yang bisa diakses oleh pihak lain. Bahkan, jika password tersebut disimpan di komputer pribadi bukan berarti orang lain tidak bisa mengakses akun tersebut, bisa jadi ketika orang lain tersebut sedang meminjam komputer pribadi *user* maka terjadi celah untuk pihak lain bisa menggunakan akun *user* pemilik komputer. Hal ini menjadi masalah ketika pihak lain sudah dapat masuk kedalam akun *user* tersebut, maka pihak lain dianggap oleh sistem sebagai pengguna yang sesungguhnya dan diijinkan untuk menginput, merubah menghapus berbagai macam data khususnya data-data yang bersifat rahasia [4]. Pada gambar 1 dapat dilihat penerapan metode 2FA dengan menggunakan paradigma model *prototyping.*

Tahapan awal pengembangan metode 2FA dengan mengadopsi paradigma model *prototyping* adalah dengan melakukan observasi lapangan terkait laporan pengguna pada isu keamanan saat *login.* Isu terkait keamanan pada proses *login* yang ditemukan dijadikan acuan untuk melakukan proses perancang dan desain metode 2FA. Metode 2FA dikembangkan menggunakan model *one time password* (OTP) berkolaborasi dengan bot Telegram dan autentikasi kalkulasi berbasis PHP sebagai langkah untuk meningkatkan keamanan sistem informasi akademik [14]. Isu kelamahan terhadap akses *login* sistem informasi akademik diharapkan dapat diantisipasi dan diminimalisirkan sedini-dininya untuk menghidari serangan lebih jauh ke dalam sistem informasi akademik [15]. Tahapan selanjutnya ialah bagaimana metode ini diterapkan dan diperkenalkan kepada pengguna agar dapat menggunakan fitur 2FA yang telah dikembangkan sebagai jawaban atas isu keamanan terhadap akses *login* sistem informasi akademik. Pada

bagian ini pengembang memberikan panduan pengguna terkait bagaimana langkah-langkah aktifasi fitur 2FA agar dapat digunakan pengguna secara mandiri.

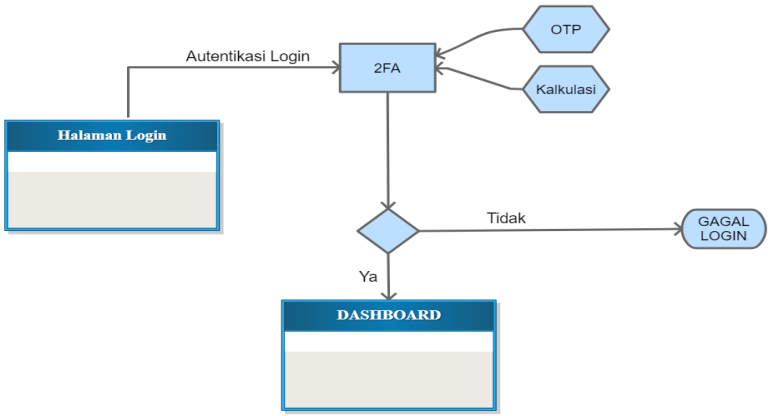


Gambar 1. Pengembangan metode 2FA dengan pendekatan model *prototyping* pada sistem informasi akademik [13]

Hasil dari pengembangan metode 2FA ini juga ditujukan untuk fleksibilitas sistem yang mengacu pada hasil evaluasi dan masukan terhadap kelanjutan pengembang sistem informasi akademik.

3. HASIL DAN PEMBAHASAN

Penelitian ini mengembangkan metode 2FA dengan model gabungan antara kalkulasi angka dan model OTP yang dikirimkan melalui pesan bot Telegram. Kalkulasi bertujuan untuk memastikan bahwa pengguna adalah manusia, sedangkan bot telegram memastikan bahwa pengguna adalah pemilik yang sah, karena OTP hanya dikirim ke telegram pemilik. Autentikasi dilakukan dengan melakukan pengecekan kedua variabel tersebut agar keamanan sistem terkait *login* akun diharapkan dapat lebih kuat dalam keamanannya agar pengguna merasakan pengalaman yang baik saat menggunakan sistem informasi akademik. Proses autentikasi akan membaca kedua variabel tersebut sehingga dapat disimpulkan jika pengguna sudah menginput kode OTP maka secara langsung sistem akan memberikan hak akses untuk ke halaman *dashboard* pengguna sistem informasi akademik. Pada gambar 2 dapat dilihat skema dari metode 2FA dengan model OTP dan autentikasi penjumlahan pada sistem informasi akademik.



Gambar 2. Skema *Two-Factor Authentication* Sistem Informasi Akademik

3.1. Aktifasi Metode *Two-Factor Authentication* (2FA)

Pada bagian ini pengembangan metode 2FA dirumuskan menggunakan bahasa pemrograman PHP sebagai bahasa pengembangan *website,* dapat dilihat pada gambar 3 sampai dengan gambar 5 *source code* program untuk mengaktifkan metode 2FA pada halaman *login* sebagai langkah pengamanan sandi dan akun pengguna.

```php
$op=rand(1,2);
if($op==1){
    $a1=rand(1,9);
    $a2=rand(1,20);
    $b=$a1+$a2;
    $kalJumlah="Berapa $a1 ditambah $a2 ?";
}else{
    $a1=rand(1,9);
    $a2=rand(1,5);
    $b=$a1*$a2;
    $kalJumlah="Berapa $a1 dikali $a2 ?";
}
```

Gambar 3. Function untuk menentukan operator dan angka kalkulasi

Pada gambar 3 dilakukan operasi acak untuk menentukan operator kalkulasi yang akan menghasilkan perkalian atau penjumlahan, kemudian setelah didapatkan operator selanjutnya menentukan angka yang akan dikalikan atau ditambah, setelah itu hasilnya disimpan dalam *server* yang kemudian akan dicocokkan sesuai dengan isian pengguna. Kalkulasi ini merupakan bagian penting juga terhadap metode 2FA karena semakin kompleks autentikasi akan semakin memberikan keamanan pada pengguna, tentunya juga akan mempersulit orang yang tidak berwenang pada akun sistem informasi akademik agar tidak dengan mudah meretas akun milik orang lain.

```php
if($d[idtel]>0 && strlen($d[idtel])>5 && $d[batastel]<$skg){
  $alphanum="1234567890";
  $pesan=substr(str_shuffle($alphanum),0,6);
  $pesan2="Kode Akses SISCA untuk username $username adalah $pesan. Expired: $tgl2 23:59:59. Jaga kerahasiaan kode ini.";
  $token = "bot".";
  $chat_id = $d[idtel];
  $url = "https://api.telegram.org/$token/sendMessage?parse_mode=markdown&chat_id=$chat_id&text=$pesan2";

  $ch = curl_init();
  if($proxy==""){
    $optArray = array(
      CURLOPT_URL => $url,
      CURLOPT_RETURNTRANSFER => true,
      CURLOPT_CAINFO => "../api/cacert.pem"
    );
  }
  else{
    $optArray = array(
      CURLOPT_URL => $url,
      CURLOPT_RETURNTRANSFER => true,
      CURLOPT_PROXY => "$proxy",
      CURLOPT_CAINFO => "../api/cacert.pem"
    );
  }

  curl_setopt_array($ch, $optArray);
  $result = curl_exec($ch);
  $err = curl_error($ch);
  curl_close($ch);


  if($err<>""){
    echo "Error: $err";
  }else{
    $batas=date("Y-m-d");
    $d=$db->save('tbl_user',[
      'kodetel'=>$pesan,
      'batastel'=>$batas
    ],[
      'idtel'=>$d[idtel],
      'username'=>$username
    ]);
  }

}
```

Gambar 4. *Function* untuk mengirimkan kode akses ke user

Kode program pada gambar 5 merupakan *function* dicek terlebih dahulu apakah pengguna sudah mengaktifkan fitur 2FA, jika sudah maka berikutnya akan dicek apakah batas OTP sudah kadaluarsa. Jika sudah kadaluarsa maka sistem akan mengirimkan OTP yang baru ke pengguna melalui bot telegram.

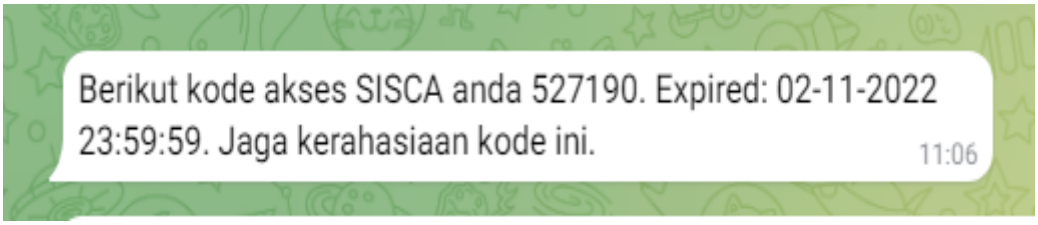
```php
<?php
session_start();
error_reporting(0);
date_default_timezone_set("asia/jakarta");
$kd=date("H");
require_once '../inc/klas.php';
if($_SESSION[auth]==md5($kd)){
  $ses=1;
}else{
  $ses=0;
}

if(!empty($_SESSION[login]) && $ses==1){
  require_once '../inc/antis.php';
  require_once '../inc/database.php';
  $id=antis($_GET[id]);
  $id=str_replace("'", "", $id);

  $db=new Database();
  $jData=0;
  $jData=$db->get("tbl_user",[
    'username'=>$_SESSION[user],
    'kodetel'=>$kodeakses
  ]);
  $d=$db->get("tbl_user",[
    'username'=>$_SESSION[user],
    'password'=>$tpassword
  ]);
  $ttoday=date('Y-m-d');
  if($d[batastel]>=$skg && $j==1){
    echo "<h1>Sukses!</h1>";
    $toktgl=date("dmY");
    echo "<script>window.location.assign('../dosen');</script>";
  }else{
    echo "<script>window.location.assign('../logout.php');</script>";
  }
?>
<div class="col-lg-12 col-md-12">
 <div class="panel panel-default">
   <div class="panel-heading">
     <h2>Verifikasi Kode Akses</h2>
   </div>
   <div class="panel-body">
     <?php
     //echo "<h1>($id)</h1>";
     ?>
   </div>
 </div>
</div>
 <?php
}else{
  echo "<script>window.location.assign('http://sisca.uinsaizu.ac.id/logout.php');</script>";
}
?>
```

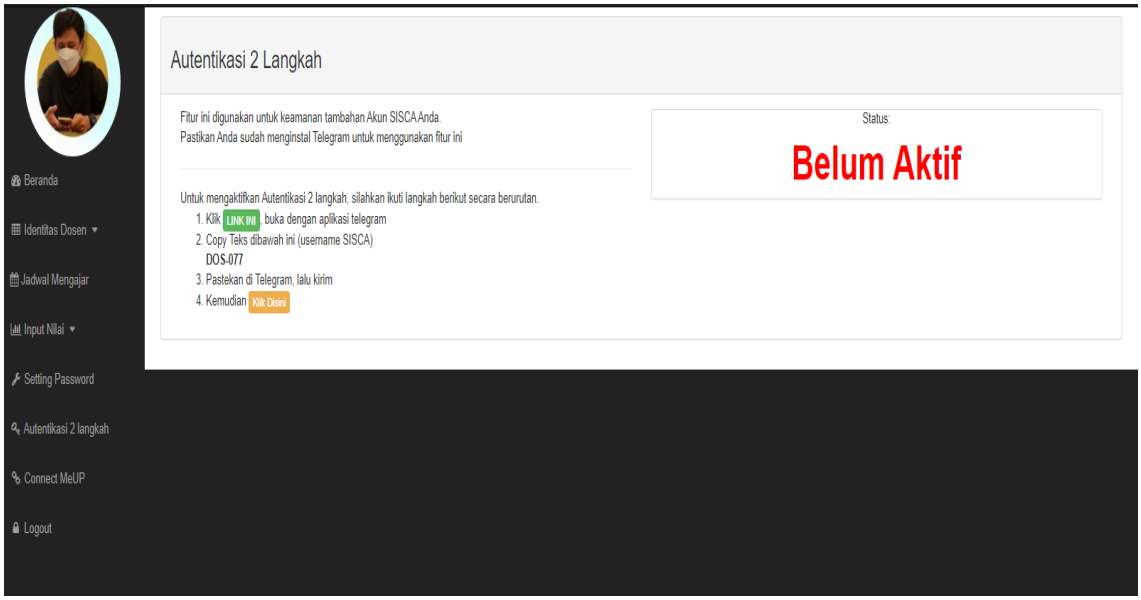
Gambar 5. *Function* untuk Pengecekkan Autentikasi

Pada gambar 6 dapat dilihat pesan yang berisi kode OTP yang diterima pengguna melalui aplikasi bot Telegram. Pengguna kemudian dapat melanjutkan proses *login* dengan cara memasukan kode OTP tersebut pada halaman *login*. Selain itu, pengguna diwajibkan menjawab pertanyaan kalkulasi untuk autentikasi selanjutnya agar memenuhi kriteria 2FA. Pengguna diwajibkan memasukan kode OTP tersebut pada saat melakukan *login* pertama kali ke sistem informasi akademik. *Function* pada PHP akan melakukan autentikasi terhadap kode OTP dan melanjutkan proses berdasarkan hasil autentikasi tersebut.



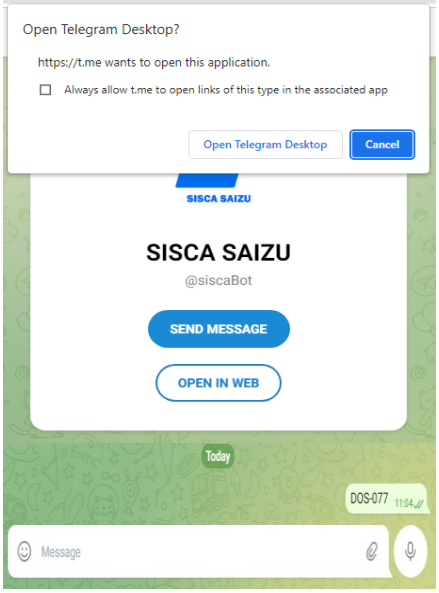
Gambar 6. Pesan dari Bot Telegram yang Memuat Kode OTP

Pesan bot Telegram yang dikirimkan melalui *server* sistem informasi akademik untuk pengguna akun berdasarkan data aktifasi *two-factor authentication* yang dipilih pengguna itu sendiri. Proses aktifasi 2FA merupakan alternatif yang diberikan oleh pihak pengembang sistem informasi akademik untuk pengguna sehingga metode ini bersifat opsional, pengguna berhak untuk tidak mengaktifkan metode karena alasan tertentu. Fitur ini dapat diaktifkan oleh pengguna ketika sudah masuk ke dalam *dashboard* sistem informasi akademik. Pada gambar 7 dapat dilihat fitur aktifasi 2FA yang dapat dipilih oleh pengguna sebagai langkah pengamanan akun yang disediakan oleh pengembang sistem informasi. Pengguna diwajibkan memiliki akun Telegram sebagai aplikasi pengiriman kode OTP. Langkah berikutnya pengguna diwajibkan memasukan kode akun mereka melalui pesan chat aplikasi Telegram dan selanjutnya proses aktifasi akan dikonfirmasi secara otomatis oleh *server* sistem informasi akademik.



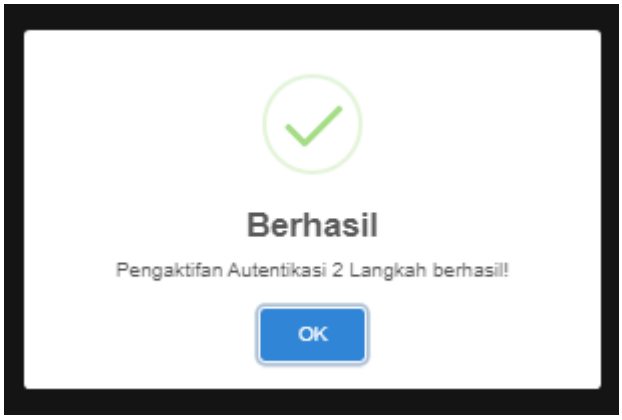
Gambar 7. Langkah Pertama untuk Aktifasi 2FA untuk Pengguna Sistem Informasi Akademik

Tahapan aktifasi selanjutnya setelah memilih untuk mengaktifkan metode login 2FA ialah sistem informasi akan secara otomatis mengarahkan langsung pengguna ke halaman Telegram untuk proses autentikasi OTP pengguna. Autentikasi OTP diaktifkan melalui fitur bot Telegram dengan memasukan *username* akun pengguna. Pada gambar 8 dapat dilihat proses aktifasi OTP menggunakan bot Telegram.

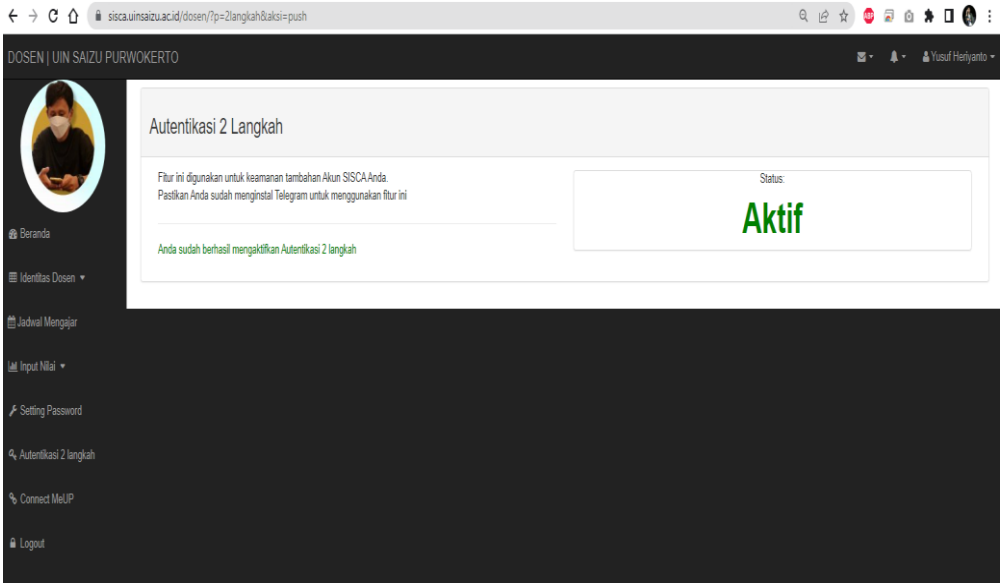


Gambar 8. Aktifasi OTP menggunakan fitur bot Telegram untuk Pengguna Sistem Informasi Akademik

Setelah proses aktifasi OTP dilakukan, maka pengguna akan diarahkan kembali ke *dashboard* sistem informasi akademik dan akan muncul pesan konfirmasi berhasil melukukan aktifasi OTP. Pada gambar 9 dan 10 dapat dilihat pesan berhasil melakukan aktifasi pada sistem informasi akademik serta status aktif 2FA pada akun pengguna. Langkah-langkah aktifasi 2FA ini perlu dipahami dan diedukasi kepada setiap pengguna karena pentinngya keamanan akun. Hal ini dapat diatasi dengan saling bersinergi antara pihak pengembang dan pengguna, karena pengembang memiliki kewajiban memberikan kualitas sistem informasi dengan performa dan keamanan yang baik, begitu pula dari sisi pengguna harus memahami bahwa tanggung jawab keamanan juga dapat dilaksanakan secara pribadi terlebih dahulu agar bisa menghindari potensi peretasan akun pengguna. Metode 2FA memenuhi sinergi kedua belah pihak yang terlibat pada sistem informasi akademik agar bisa terus saling perduli akan pentingnya keamanan bersama.



Gambar 9. Pesan Konfirmasi Berhasil Melakukan Aktifasi OTP menggunakan fitur bot Telegram untuk Pengguna Sistem Informasi Akademik

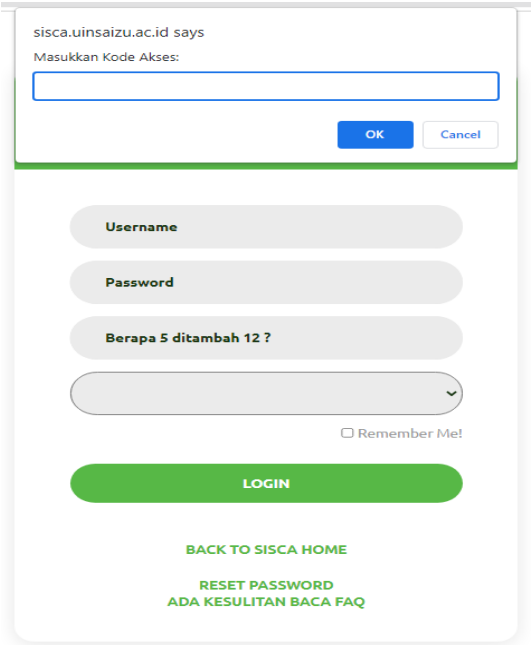


Gambar 10. Status 2FA Akun Pengguna Aktif pada Sistem Informasi Akademik

3.2. Tampilan *Two-Factor Authentication* pada Halaman *Login*

Pada bagian ini halaman login ditampilkan pada pengguna untuk memasukan sandi dan akun pengguna. Metode 2FA yang dikembangkan ke dalam sistem informasi akademik menambahkan fitur autentikasi pengguna dengan diwajibkan menjawab pertanyaan penjumlahan yang tertera secara acak dan wajib memasukan kode OTP yang diterima pengguna pada aplikasi Telegram. Sistem informasi akademik selanjutnya akan melakukan autentikasi secara otomatis dengan membaca semua variabel yang sudah diisi oleh pengguna. Proses ini yang menentukan secara otomatis apakah pengguna dapat masuk untuk lanjut ke dashboard sistem atau tertolak karena proses autentikasi tidak sesuai.

Pada gambar 11 dapat kita lihat tampilan dari halaman login sistem informasi akademik yang sudah dikembangkan dengan metode 2FA. Hal ini diharapkan dapat membantu pengguna untuk menjaga keamanan sandi dan akun mereka serta menghindari kelalaian pengguna terhadap sandi dan akun mereka.



Gambar 11. Tampilan *Login* menggunakan Metode 2FA

Pengguna diwajibkan mengisi kode OTP yang diterima melalui bot Telegram yang nantinya akan dicocokan secara otomatis melalui program PHP yang dibangun untuk mengidentifikasi pengguna asli akun sistem informasi akademik. Kemudian, autentikasi kalkulasi juga merupakan bagian penting yang tak terpisahkan dalam pengembangan metode 2FA. Pengguna dapat identifikasi dengan autentikasi kalkulasi untuk menghidari serangan *bruteforce* yang sering terjadi terhapap sistem informasi [16] [17]. Celah untuk masuknya peretas dapat diminimalisir dengan adanya kedua langkah autentikasi yang diterapkan pada sistem informasi akademik. Selain metode 2FA, sistem informasi akademik juga telah dilengkapi fitur memilih jenis akun, ini berguna untuk melakukan klasifikasi pengguna pada sistem informasi akademik sekaligus dapat dijadikan metode keamanan tambahan untuk menunjang kualitas keamanan sistem informasi akademik.

4. KESIMPULAN

Isu keamanan sistem informasi menjadi perhatian penting bagi semua pengembang sistem informasi. Kelemahan keamanan tersebut bisa terjadi karna kelalaian pribadi ataupun serangan dari pihak lain yang memiliki tujuan tersendiri terhadap performa sistem informasi [4]. Penelitian ini mengambil isu kelalaian pengguna terhadap keamanan keamanan akun mereka. Banyak aplikasi *browser* memiliki kemampuan untuk menyimpan akses *login* pengguna dengan tujuan agar mempercepat akses ketika login dan menghindari lupa password, namun fitur ini menjadi celah yang ditemukan oleh para pengembang dan pihak lain yang tidak bertanggung jawab sehingga perlu adanya solusi untuk meminimalisir kelemahan tersebut. Kelemahan pada sisi keamanan baik itu dari sisi pengembang serta dari sisi pengguna merupakan isu-isu yang terus menjadi wacana pada proses perjalanan sebuah sistem informasi. Peneliti melihat butuhnya sebuah tindakan cepat tanggap terkait isu-isu tersebut guna menghindari resiko-resiko yang dapat terjadi kedepannya.

Penelitian ini mengusulkan metode *two-factor authentication* (2FA) untuk dapat menjadi solusi alternatif untuk mencegah kelalaian pengguna. Penerapan metode 2FA dengan kolaborasi bot Telegram sebagai aplikasi untuk pengiriman kode *one time password* (OTP) guna proses autentikasi awal ketika pengguna akan melakukan *login* ke dalam sistem informasi akademik. Metode ini ditujukan agar pengguna dapat lebih waspada dan keamanan akun pengguna lebih terjamin ketika proses *login* diwajibkan untuk mengirimkan pesan OTP yang diterima di aplikasi Telegram pengguna. Metode login dengan proses autentikasi kalkulasi yang wajib dimasukan oleh pengguna merupakan bagian dari pengembangan metode 2FA agar sistem informasi semakin memberikan kualitas keamanan sistem yang baik itu dari sisi pengembang ataupun dari pihak pengguna. Hasil pengembangan metode 2FA pada penelitian ini sudah diterapkan secara langsung kepada pengguna dengan memberikan panduan aktifasi metode 2FA.

Penelitian ini juga ditujukan agar kedepannnya dapat menginspirasi serta memotivasi para pengembang sistem informasi untuk bisa memberikan solusi-solusi alternatif lain terkait isu-isu keamanan pada sistem infomasi.

DAFTAR PUSTAKA

[1] Government of Japan, "Realizing Society 5.0," *NewsPick Brand Des.*, 2018, [Online]. Available: https://www.japan.go.jp/abenomics/_userdata/abenomics/pdf/society_5.0.pdf.

[2] M. K. Sharma and M. J. Nene, "Two-factor authentication using biometric based quantum operations," *Secur. Priv.*, vol. 3, no. 3, 2020, doi: 10.1002/spy2.102.

[3] H. Tabrizchi and M. K. Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," *Springer Sci. Media*, 2020.

[4] T. Petsas, G. Tsirantonakis, E. Athanasopoulos, and S. Ioannidis, "Two-factor Authentication : Is the World Ready ? Quantifying 2FA Adoption Categories and Subject Descriptors," *Proc. Eighth Eur. Work. Syst. Secur.*, no. April, pp. 1–7, 2015, [Online]. Available: google.com.

[5] K. C. Laudon and J. Laudon, *IT Infrastructure and Emerging Technologies*. 2018.

[6] C. Z. Acemyan, P. Kortum, J. Xiong, and D. S. Wallach, "2FA might be secure, but it's not usable: A summative usability assessment of Google's two-factor authentication (2FA) methods," *Proc. Hum. Factors Ergon. Soc.*, vol. 2, pp. 1141–1145, 2018, doi: 10.1177/1541931218621262.

[7] D. Wang, Q. Gu, H. Cheng, and P. Wang, "The request for better measurement: A comparative evaluation of two-factor authentication schemes," *ASIA CCS 2016 - Proc. 11th ACM Asia Conf. Comput. Commun. Secur.*, no. May, pp. 475–486, 2016, doi: 10.1145/2897845.2897916.

[8] P. Gope and B. Sikdar, "Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, 2019, doi: 10.1109/JIOT.2018.2846299.

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

[10] N. Karapanos *et al.*, "Sound-Proof : Usable Two-Factor Authentication Based on Ambient Sound This paper is included in the Proceedings of the," *Usenix Secur.*, 2015.

[11] N. Morze, O. Buinytska, and L. Varchenko-Trotsenko, "Use of Bot-Technologies for Educational Communication At the University," *Eff. Dev. Teach. Ski. Area Ict E-Learning*, vol. 9, pp. 239–248, 2017, [Online]. Available: https://depot.ceon.pl/handle/123456789/15492.

[12] Telegram, "Telegram Bot API," 2022. https://core.telegram.org/bots/api.

[13] R. S. Pressman and B. R. Maxim, *Software Engineering A PRACTITIONER'S APPROACH*. McGraw-Hill, 2020.

[14] D. E. Kurniawan, M. Iqbal, J. Friadi, F. Hidayat, and R. D. Permatasari, "Login Security Using One Time Password (OTP) Application with Encryption Algorithm Performance," *J. Phys. Conf. Ser.*, vol. 1783, no. 1, 2021, doi: 10.1088/1742-6596/1783/1/012041.

[15] H. Khalid, S. J. Hashim, S. M. S. Ahmad, F. Hashim, and M. A. Chaudary, "New and Simple Offline Authentication Approach using Time-based One-time Password with Biometric for Car Sharing Vehicles," *2020 IEEE Asia-Pacific Conf. Comput. Sci. Data Eng. CSDE 2020*, no. April 2021, 2020, doi: 10.1109/CSDE50874.2020.9411569.

[16] C. Adams, G. V. Jourdan, J. P. Levac, and F. Prevost, "Lightweight protection against brute force login attacks on web applications," *PST 2010 2010 8th Int. Conf. Privacy, Secur. Trust*, pp. 181–188, 2010, doi: 10.1109/PST.2010.5593241.

[17] F. Ayankoya and B. Ohwo, "Brute-Force Attack Prevention in Cloud Computing Using One-Time Password and Cryptographic Hash Function," *Int. J. Comput. Sci. Inf. Secur.*, vol. 17, no. 2, pp. 7–19, 2019, [Online]. Available: https://www.academia.edu/38523734/Brute-Force_Attack_Prevention_in_Cloud_Computing_Using_One-Time_Password_and_Cryptographic_Hash_Function.