JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Analisis Sistem Autentikasi Dua Faktor (2FA) Dan Efektivitasnya Dalam Meningkatkan Keamanan Akses

Azkal Azkiya[1*], Muhammad Budi Prayoga Ichsan[2], Nabil Azhari Putra Finula Hasibuan[3], Reva Andrianti[4], Intan Maulana[5]
[1,2,3,4,5]Universitas Malikussaleh, Indonesia
[1]azkal.240170235@mhs.unimal.ac.id,[2]muhammad.240170042@mhs.unimal.ac.id,[3]nabil.240170025@mhs.unimal.ac.id,
[4]reva.240170056@mhs.unimal.ac.id, [5]intan240170049@mhs.unimal.ac.id

ABSTARCT

The rapid development of information technology has led to an increase in security threats to digital systems, particularly in user authentication mechanisms. Single-factor authentication based solely on passwords is no longer sufficient to protect system access from attacks such as phishing, brute force, and credential stuffing. Therefore, two-factor authentication (2fa) has emerged as a solution by adding an additional layer of security. This study aims to analyze the concept of 2fa and evaluate its effectiveness in improving system access security. The research method used is a literature study of various studies and implementations of 2fa in modern information systems. The results indicate that the implementation of 2fa significantly reduces the risk of unauthorized access and increases user trust in system security, despite challenges related to usability and technical implementation.

Keywords:
Authentication, Two-Factor Authentication, System Security, Information Systems

PENDAHULUAN

Era digital yang dikenal sebagai era *Society 5.0* merupakan sebuah upaya manusia dalam memanfaatkan teknologi untuk mempermudah berbagai aktivitas secara daring. Perkembangan era digital ini membawa perubahan yang signifikan dalam dunia pendidikan, khususnya dalam peningkatan kualitas layanan dan proses pembelajaran, sehingga secara bertahap mampu mengurangi keterbatasan metode pembelajaran dan pelayanan tradisional. Transformasi layanan ke platform daring yang semakin masif turut meningkatkan kebutuhan akan sistem autentikasi yang lebih andal. Pengguna kini dituntut untuk mengelola serta mengingat berbagai kata sandi yang digunakan pada beragam layanan digital. Meskipun perangkat lunak peramban dengan fitur pengelola kata sandi dapat menjadi solusi, beberapa penelitian menyimpulkan bahwa penggunaan pengelola kata sandi justru dapat memperburuk kondisi keamanan pada situasi tertentu. Selain itu, kebiasaan pengguna dalam memanfaatkan fitur penyimpanan kata sandi pada peramban berpotensi menimbulkan risiko serius, terutama ketika aplikasi tersebut digunakan pada perangkat yang bukan milik pribadi.

Sebagai upaya untuk mengatasi permasalahan tersebut, metode keamanan *two-factor authentication* (2FA) diusulkan guna memperkuat sistem autentikasi dari sisi server serta mencegah terjadinya pencurian kata sandi. Dalam konteks pendidikan, sistem informasi akademik yang berperan sebagai media pelayanan dan pembelajaran memerlukan terobosan baru terkait aspek keamanan sistem. Hal ini disebabkan oleh besarnya volume data yang tersimpan dalam sistem informasi akademik, yang sebagian besar bersifat pribadi dan rahasia. Oleh karena itu, potensi celah keamanan yang dapat membuka peluang terjadinya kejahatan siber harus diantisipasi sejak dini. Meskipun pengembang sistem terus berupaya meningkatkan keamanan, rancangan sistem 2FA yang aman sekaligus efisien masih menjadi permasalahan terbuka yang memerlukan kajian lebih lanjut.

Pengembangan sistem keamanan melalui penerapan metode 2FA dengan memanfaatkan *one time password* (OTP) yang dikirim melalui aplikasi Telegram serta autentikasi berbasis kalkulasi diusulkan sebagai langkah awal pencegahan terhadap serangan siber. Pendekatan ini merupakan bentuk perlindungan keamanan berlapis yang bertujuan meminimalkan akses tidak sah terhadap akun pengguna, sehingga dapat mempersulit upaya pelaku kejahatan siber dalam menembus sistem informasi. Selain itu, metode ini diharapkan mampu memberikan manfaat bagi pengguna dan pengembang sistem dalam menjaga kerahasiaan data serta mencegah akses oleh pihak yang tidak berwenang.

Berbagai penelitian sebelumnya telah membahas penerapan metode 2FA pada sistem informasi. Salah satunya adalah penggunaan *physically unclonable functions* (PUFs) yang terbukti mampu meningkatkan ketahanan dan efisiensi sistem terhadap serangan siber. Penelitian lainnya mengombinasikan PUFs dengan *voiceprint* dalam metode *transparent two-factor authentication* (T2FA) untuk memberikan kenyamanan sekaligus keamanan bagi pengguna dalam berinteraksi di lingkungan digital. Selain itu, terdapat pula pengembangan model keamanan berbasis *sound-proof* yang dapat diimplementasikan dengan mudah melalui smartphone dan peramban tanpa memerlukan plugin tambahan. Beragam penelitian tersebut menunjukkan bahwa metode 2FA memiliki potensi besar dalam meningkatkan keamanan sistem informasi.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Penelitian ini mengusulkan penerapan metode 2FA sebagai solusi terhadap tantangan keamanan pada sistem informasi akademik. Implementasi metode ini difokuskan pada tahap awal penggunaan sistem guna mencegah potensi serangan siber sebelum pelaku berhasil mengakses dashboard pengguna. Aplikasi pesan instan Telegram dipilih sebagai media pengiriman OTP karena tingkat popularitas dan penggunaannya yang luas di kalangan masyarakat modern. Selain itu, Telegram menyediakan fasilitas *bot Application Programming Interface* (API) dengan dokumentasi yang lengkap serta bersifat gratis, sehingga mendukung otomasi pengiriman pesan secara efisien. Pemanfaatan teknologi bot ini dinilai mampu meningkatkan keandalan proses autentikasi dalam mengidentifikasi pengguna secara akurat.
Dengan mengombinasikan metode 2FA, OTP berbasis Telegram, serta autentikasi kalkulasi, sistem keamanan pada sistem informasi akademik diharapkan dapat ditingkatkan secara signifikan. Pendekatan ini diharapkan tidak hanya mampu melindungi data dan akun pengguna dari akses tidak sah, tetapi juga memberikan rasa aman dan kenyamanan bagi pengguna sebagai bentuk tanggung jawab pengembang dalam menjaga keamanan sistem informasi akademik.

TINJAUAN PUSTAKA

Keamanan sistem informasi merupakan aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data. Salah satu komponen utama dalam keamanan sistem adalah mekanisme autentikasi, yang berfungsi untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sistem. Autentikasi yang lemah dapat menjadi celah keamanan yang dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan penyalahgunaan data dan akses ilegal. Pada sistem informasi modern, ketergantungan terhadap layanan digital menyebabkan pengguna harus mengelola banyak akun dengan kredensial yang berbeda. Kondisi ini meningkatkan risiko penggunaan kata sandi yang lemah, berulang, atau disimpan secara tidak aman. Oleh karena itu, sistem autentikasi tidak lagi cukup hanya mengandalkan satu faktor seperti username dan password.

Untuk mengatasi permasalahan tersebut, dikembangkan metode autentikasi berlapis yang mengombinasikan lebih dari satu faktor verifikasi. Autentikasi dua faktor (Two-Factor Authentication/2FA) menjadi salah satu pendekatan yang banyak diterapkan karena mampu meningkatkan keamanan akses dengan menambahkan faktor verifikasi tambahan. Penerapan 2FA diharapkan dapat meminimalkan risiko akses tidak sah dan meningkatkan perlindungan terhadap data yang bersifat sensitif, khususnya pada sistem informasi akademik.

Konsep Autentikasi

Autentikasi merupakan proses verifikasi yang dilakukan oleh sistem untuk memastikan bahwa pengguna yang mencoba mengakses suatu sistem benar-benar pihak yang berwenang. Proses ini menjadi bagian penting dalam keamanan sistem informasi karena berfungsi sebagai gerbang awal sebelum pengguna dapat mengakses data atau layanan tertentu. Tanpa mekanisme autentikasi yang baik, sistem informasi sangat rentan terhadap penyalahgunaan dan akses tidak sah. Secara umum, autentikasi dilakukan dengan mencocokkan identitas pengguna dengan kredensial yang dimiliki, seperti username dan password. Metode ini dikenal sebagai autentikasi berbasis pengetahuan (something you know). Namun, penggunaan autentikasi tunggal seperti password memiliki banyak kelemahan, di antaranya password mudah ditebak, dicuri, atau disimpan secara tidak aman oleh pengguna, misalnya melalui browser atau perangkat umum. Seiring meningkatnya ancaman keamanan siber, konsep autentikasi terus berkembang. Autentikasi tidak hanya berfungsi untuk mengenali identitas pengguna, tetapi juga sebagai upaya perlindungan data dan menjaga kerahasiaan informasi. Oleh karena itu, diperlukan metode autentikasi yang lebih kuat dan berlapis agar keamanan sistem informasi dapat ditingkatkan secara optimal.

Autentikasi Dua Faktor

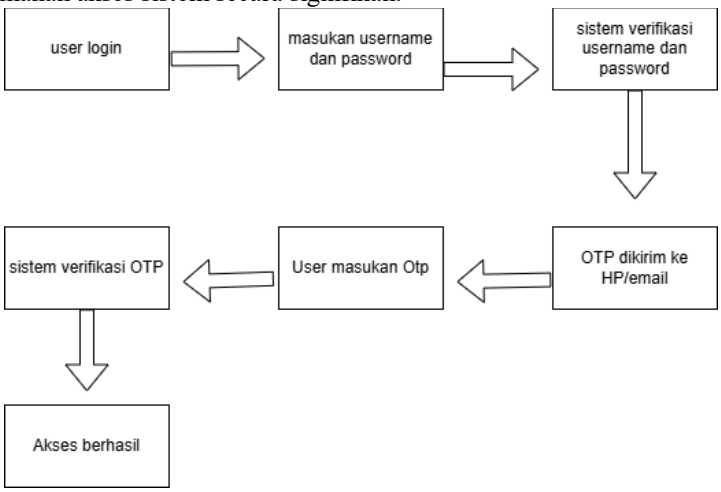
Autentikasi dua faktor atau Two-Factor Authentication (2FA) merupakan metode keamanan yang menggabungkan dua jenis verifikasi berbeda dalam proses login pengguna. Metode ini dirancang untuk meningkatkan keamanan sistem dengan cara tidak hanya bergantung pada satu faktor autentikasi saja, seperti password. Dengan 2FA, meskipun password diketahui oleh pihak yang tidak berwenang, sistem tetap tidak dapat diakses tanpa faktor kedua. Pada umumnya, autentikasi dua faktor mengombinasikan dua dari tiga kategori autentikasi, yaitu sesuatu yang diketahui pengguna (something you know) seperti password, sesuatu yang dimiliki pengguna (something you have) seperti kode OTP yang dikirim ke ponsel atau aplikasi pesan, dan sesuatu yang melekat pada pengguna (something you are) seperti sidik jari atau biometrik. Kombinasi ini membuat proses login menjadi lebih aman karena mempersulit upaya peretasan. Penerapan 2FA banyak digunakan pada sistem informasi yang menyimpan data penting dan bersifat rahasia, termasuk sistem informasi akademik. Penggunaan One Time Password (OTP) sebagai faktor kedua menjadi solusi yang cukup efektif karena kode yang dikirim bersifat sementara dan hanya dapat digunakan satu kali. Dengan demikian, autentikasi dua faktor mampu meminimalisir risiko pencurian akun akibat kelalaian pengguna maupun serangan siber, serta memberikan perlindungan keamanan yang lebih baik dibandingkan autentikasi satu faktor.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Alur OTP

Dalam penerapan autentikasi dua faktor (Two-Factor Authentication/2FA), penggunaan One Time Password (OTP) berperan sebagai lapisan keamanan tambahan setelah proses autentikasi utama menggunakan username dan password. OTP dirancang sebagai kode autentikasi bersifat sementara yang hanya dapat digunakan satu kali dan dalam jangka waktu tertentu. Karakteristik ini bertujuan untuk mengurangi risiko penyalahgunaan kredensial, khususnya apabila kata sandi utama diketahui atau dicuri oleh pihak yang tidak berwenang.

Secara umum, mekanisme OTP bekerja dengan menghasilkan kode unik yang dikirimkan kepada pengguna melalui media komunikasi yang telah terdaftar, seperti email atau aplikasi pesan instan. Sistem kemudian melakukan verifikasi terhadap kode tersebut berdasarkan kecocokan nilai dan batas waktu penggunaan. Pendekatan ini memastikan bahwa akses sistem tidak hanya bergantung pada informasi yang diketahui pengguna, tetapi juga pada kepemilikan perangkat atau akun penerima OTP. Dengan demikian, integrasi OTP dalam sistem autentikasi dua faktor diharapkan mampu meningkatkan keamanan akses sistem secara signifikan.



Gambar 1. Diagram Alur Autentikasi Dua Faktor (2FA) Menggunakan One Time Password (OTP)

Dari gambar 1 menunjukkan alur proses autentikasi dua faktor (2FA) menggunakan One Time Password (OTP). Proses diawali dengan pengguna melakukan login menggunakan username dan password. Sistem kemudian melakukan verifikasi terhadap kredensial tersebut. Apabila username dan password valid, sistem akan mengirimkan kode OTP ke perangkat pengguna melalui media yang telah ditentukan, seperti email atau aplikasi pesan instan.

Selanjutnya, pengguna memasukkan kode OTP yang diterima ke dalam sistem. Sistem akan melakukan verifikasi terhadap OTP yang dimasukkan berdasarkan kecocokan kode dan batas waktu yang telah ditentukan. Jika OTP valid dan masih dalam masa berlaku, maka sistem memberikan akses kepada pengguna. Sebaliknya, apabila OTP tidak valid atau telah melewati batas waktu, maka proses autentikasi gagal dan pengguna diminta untuk mengulangi proses login.

Alur ini menunjukkan bahwa penerapan OTP sebagai faktor autentikasi kedua mampu meningkatkan keamanan akses sistem dengan menambahkan lapisan verifikasi tambahan setelah proses login utama. Dengan demikian, risiko akses tidak sah akibat pencurian username dan password dapat diminimalisir.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan rekayasa perangkat lunak dengan menerapkan model pengembangan prototyping dalam merancang dan mengimplementasikan sistem keamanan Two-Factor Authentication (2FA) pada sistem informasi akademik. Pendekatan ini dipilih karena mampu memberikan gambaran awal sistem kepada pengguna serta memungkinkan pengembangan dilakukan secara bertahap berdasarkan hasil evaluasi dan umpan balik.Tahap awal penelitian diawali dengan identifikasi permasalahan melalui observasi terhadap proses autentikasi login serta analisis laporan pengguna terkait keamanan sistem. Hasil observasi menunjukkan adanya potensi kerentanan akibat kebiasaan pengguna menyimpan kata sandi pada peramban atau menggunakan perangkat bersama, sehingga meningkatkan risiko akses tidak sah ke akun pengguna.

Berdasarkan permasalahan tersebut, dilakukan perancangan solusi keamanan berupa penerapan mekanisme autentikasi berlapis. Sistem 2FA dikembangkan sebagai lapisan keamanan tambahan setelah proses autentikasi utama menggunakan username dan password. Metode ini bertujuan untuk meminimalkan risiko penyalahgunaan akun meskipun kredensial utama diketahui oleh pihak lain.

Pengembangan sistem dilakukan mengikuti tahapan model prototyping yang meliputi: komunikasi kebutuhan, perencanaan awal, perancangan cepat, pembangunan prototipe, serta implementasi dan evaluasi. Pada tahap komunikasi, peneliti menggali kebutuhan pengguna dan pengelola sistem terkait fitur keamanan login. Tahap

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

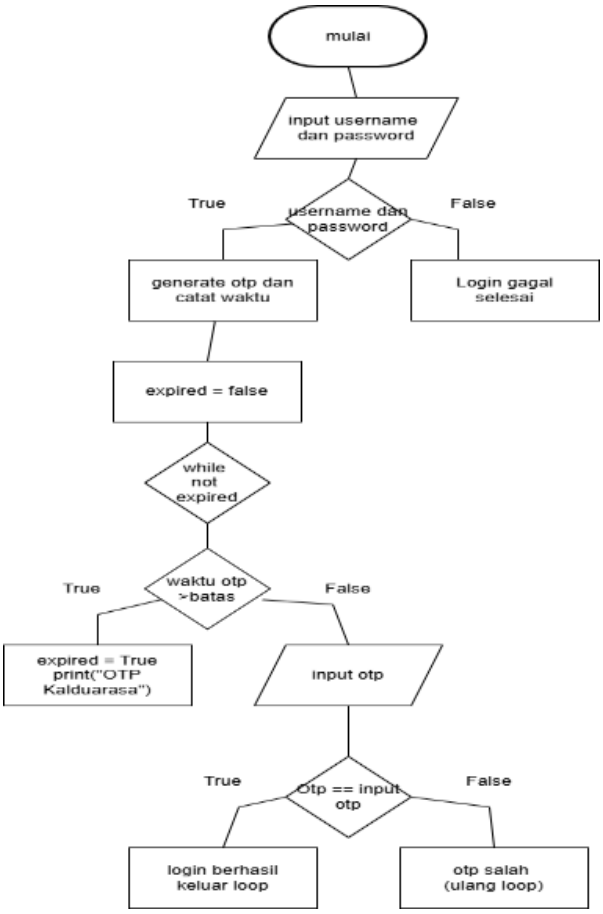
perencanaan dan perancangan difokuskan pada penyusunan alur autentikasi 2FA yang sederhana namun efektif.

Implementasi 2FA dilakukan menggunakan metode One Time Password (OTP) sebagai faktor autentikasi kedua. Kode OTP dihasilkan secara dinamis dan dikirimkan kepada pengguna melalui layanan bot Telegram, kemudian diverifikasi oleh sistem menggunakan mekanisme autentikasi berbasis waktu. Sistem dikembangkan menggunakan bahasa pemrograman PHP dan diintegrasikan langsung dengan modul login sistem informasi akademik yang telah ada.
Tahap akhir penelitian melibatkan pengujian dan evaluasi sistem untuk menilai efektivitas penerapan 2FA dalam meningkatkan keamanan login serta kemudahan penggunaan oleh pengguna. Evaluasi dilakukan berdasarkan keberhasilan autentikasi, respon pengguna, serta kemampuan sistem dalam mencegah akses tidak sah. Hasil evaluasi selanjutnya digunakan sebagai dasar penyempurnaan sistem hingga diperoleh solusi keamanan yang optimal.

HASIL DAN PEMBAHASAN

Implementasi

Implementasi yang digunakan dalam penelitian ini adalah One Time Password (OTP) sebagai faktor autentikasi kedua dalam sistem autentikasi dua faktor. Implementasi yang ditampilkan berupa simulasi sederhana untuk menggambarkan alur kerja OTP dalam proses login. Simulasi ini bertujuan untuk menunjukkan mekanisme pembuatan, pengiriman, dan verifikasi OTP dalam batas waktu tertentu. Untuk memperjelas proses tersebut, digunakan diagram alur (flowchart) yang menggambarkan tahapan autentikasi OTP secara sistematis.



Gambar 2. Flowchart Proses Autentikasi Menggunakan One Time Password (OTP)

Gambar 2 menunjukkan flowchart proses autentikasi menggunakan One Time Password (OTP) sebagai faktor autentikasi kedua. Proses diawali dengan pengguna memasukkan username dan password ke dalam sistem. Sistem kemudian melakukan verifikasi terhadap kredensial tersebut. Apabila username dan password tidak valid, maka proses login dinyatakan gagal dan sistem akan menghentikan proses autentikasi.

Jika kredensial dinyatakan valid, sistem akan menghasilkan kode OTP dan mengaktifkan batas waktu penggunaan OTP. Selanjutnya, pengguna diminta untuk memasukkan kode OTP yang diterima. Sistem akan memeriksa apakah OTP masih berada dalam masa berlaku. Apabila OTP telah melewati batas waktu, sistem akan menyatakan OTP kedaluwarsa dan meminta pengguna untuk mengulangi proses login.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Apabila OTP masih dalam batas waktu, sistem akan melakukan verifikasi kecocokan antara kode OTP yang dimasukkan pengguna dengan kode OTP yang dihasilkan sistem. Jika kode sesuai, maka autentikasi dinyatakan berhasil dan pengguna memperoleh akses ke sistem. Sebaliknya, jika kode OTP tidak sesuai, sistem akan menolak autentikasi dan meminta pengguna untuk kembali memasukkan kode OTP yang benar.

Cuplikan kode program simulasi OTP:

```python
import random
import time

def generate_otp():
    return str(random.randint(100000, 999999))

def login_system():
    username = input("Masukkan username: ")
    password = input("Masukkan password: ")

    if username == "123" and password == "123":
        print("Password benar ")

        otp = generate_otp()
        print(f"OTP kamu: {otp} (berlaku 10 detik)")

        start_time = time.time()
        expired = False

        while not expired:
            if time.time() - start_time > 10:
                print("OTP kedaluwarsa! ")
                expired = True
                break

            input_otp = input("Masukkan OTP: ")
            if time.time() - start_time > 10:
                print("OTP kedaluwarsa! ")
                expired = True
                break

            if input_otp == otp:
                print("Login berhasil! ")
                break
            else:
                print("OTP salah! ")
    else:
        print("Username atau password salah ")

login_system()
```

Gambar 3. Cuplikan Kode Program Simulasi One Time Password (OTP)

Gambar 3 menunjukkan cuplikan kode program yang digunakan untuk mensimulasikan mekanisme One Time Password (OTP). Pada simulasi ini, sistem menghasilkan kode OTP secara acak dengan jumlah digit tertentu dan menetapkan batas waktu penggunaan selama 10 detik. Setelah kode OTP dihasilkan, pengguna diminta untuk memasukkan kode tersebut ke dalam sistem.

Sistem kemudian melakukan pengecekan terhadap dua kondisi, yaitu kecocokan kode OTP dan batas waktu penggunaan. Apabila pengguna memasukkan kode OTP yang benar dan masih berada dalam batas waktu, maka proses autentikasi dinyatakan berhasil. Sebaliknya, apabila kode OTP salah atau telah melewati batas waktu yang ditentukan, sistem akan menolak autentikasi dan menampilkan pesan kesalahan. Simulasi ini digunakan untuk menggambarkan prinsip kerja OTP dalam sistem autentikasi dua faktor secara sederhana.

Dari hasil kode program di gambar 3 kita mendapatkan beberapa hasil berikut.

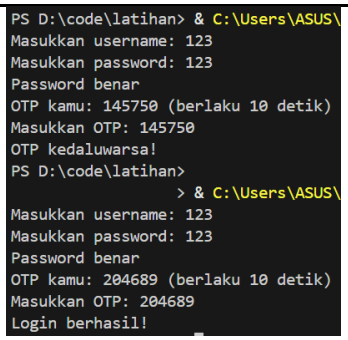
```
Masukkan username: 123
Masukkan password: 123
Password benar
OTP kamu: 768797 (berlaku 10 detik)
Masukkan OTP: 768797
Login berhasil!
```

Gambar 4. Proses Verifikasi OTP yang Valid dalam Batas Waktu

Gambar 4 menunjukkan proses verifikasi OTP ketika pengguna berhasil memasukkan kode OTP yang benar dan masih berada dalam batas waktu yang ditentukan. Sistem melakukan pencocokan antara kode OTP yang diinput oleh pengguna dengan kode OTP yang dihasilkan sebelumnya. Apabila kode sesuai dan belum kedaluwarsa, sistem memberikan akses login kepada pengguna.

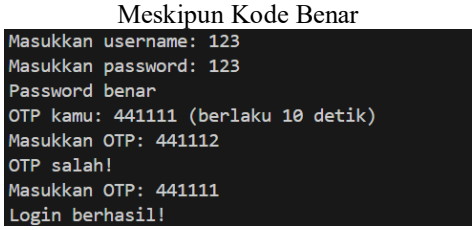
JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026



Gambar 5. Hasil Autentikasi OTP Kedaluwarsa Meskipun Kode Benar

Gambar 5 menunjukkan kondisi ketika pengguna memasukkan kode One Time Password (OTP) yang benar, namun telah melewati batas waktu penggunaan yang telah ditentukan oleh sistem. Dalam kondisi ini, sistem menolak proses autentikasi dan menyatakan OTP tidak valid. Hasil ini menunjukkan bahwa OTP bersifat sementara dan hanya dapat digunakan dalam jangka waktu tertentu sebagai mekanisme pengamanan tambahan dalam sistem autentikasi dua faktor.



Gambar 6. Kesalahan Input OTP dalam Batas Waktu Autentikasi

Gambar 6 menunjukkan kondisi ketika pengguna salah memasukkan kode One Time Password (OTP) pada percobaan pertama, namun masih berada dalam batas waktu penggunaan yang ditentukan oleh sistem. Sistem memberikan kesempatan kepada pengguna untuk kembali memasukkan kode OTP yang benar. Pada percobaan selanjutnya, autentikasi berhasil dilakukan, yang menegaskan bahwa sistem tetap menerapkan batas waktu OTP sekaligus memverifikasi keakuratan kode sebelum memberikan akses.

Kelebihan dan Kekurangan

Kelebihan

Berdasarkan implementasi yang dilakukan, penggunaan One Time Password (OTP) sebagai faktor autentikasi kedua memiliki beberapa kelebihan. Penerapan OTP mampu meningkatkan tingkat keamanan sistem karena menambahkan lapisan verifikasi tambahan selain username dan password. Dengan mekanisme ini, meskipun kredensial utama diketahui oleh pihak lain, akses sistem tetap tidak dapat dilakukan tanpa kode OTP yang valid. Hal ini menjadikan sistem lebih tahan terhadap serangan seperti pencurian kata sandi dan akses tidak sah.

Selain itu, OTP bersifat sementara dan hanya berlaku dalam jangka waktu tertentu. Kode OTP yang tidak digunakan dalam periode waktu yang telah ditentukan akan otomatis kedaluwarsa dan tidak dapat digunakan kembali. Sifat sementara ini mengurangi risiko penyalahgunaan kode autentikasi, terutama apabila kode tersebut diketahui oleh pihak lain setelah masa berlakunya berakhir. OTP juga bersifat unik karena dihasilkan secara acak dengan jumlah digit tertentu, sehingga sangat sulit untuk ditebak. Keunikan ini memperkecil kemungkinan keberhasilan serangan brute force dalam menebak kode autentikasi yang valid.

Kekurangan

Meskipun memiliki kelebihan dalam meningkatkan keamanan, penggunaan OTP juga memiliki beberapa kekurangan. Salah satu kekurangannya adalah adanya tambahan langkah dalam proses login. Pengguna tidak hanya perlu memasukkan username dan password, tetapi juga harus menunggu dan memasukkan kode OTP. Proses ini dapat menyebabkan waktu login menjadi lebih lama dan berpotensi mengurangi kenyamanan pengguna, terutama bagi sistem yang sering diakses.

Selain itu, OTP masih memiliki kemungkinan untuk dicuri, khususnya pada saat proses pengiriman kode melalui media komunikasi seperti email atau aplikasi pesan instan. Apabila kode OTP berhasil diambil oleh pihak yang tidak berwenang sebelum digunakan oleh pengguna, maka kode tersebut dapat disalahgunakan untuk mengakses sistem. Kekurangan lainnya adalah ketergantungan pada sinkronisasi waktu, terutama pada OTP berbasis waktu. Apabila terjadi perbedaan waktu antara sistem dan perangkat pengguna, maka OTP dapat kedaluwarsa lebih cepat sehingga menyebabkan kegagalan autentikasi meskipun pengguna memasukkan kode yang benar.

KESIMPULAN

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa sistem autentikasi berbasis kata sandi tunggal (single-factor authentication) memiliki berbagai kelemahan yang berpotensi dimanfaatkan dalam serangan siber, seperti pencurian kata sandi, brute force, dan akses tidak sah. Kondisi ini menunjukkan bahwa mekanisme autentikasi konvensional tidak lagi memadai untuk melindungi sistem informasi yang menyimpan data penting dan bersifat rahasia, khususnya pada sistem informasi akademik. Penerapan autentikasi dua faktor (Two-Factor

Authentication/2FA) dengan memanfaatkan One Time Password (OTP) terbukti mampu meningkatkan tingkat keamanan akses sistem. Penambahan faktor autentikasi kedua setelah proses verifikasi username dan password memberikan lapisan perlindungan tambahan yang dapat meminimalisir risiko akses tidak sah, meskipun kredensial utama pengguna telah diketahui oleh pihak lain. Karakteristik OTP yang bersifat sementara, unik, dan hanya dapat digunakan dalam jangka waktu tertentu menjadikannya efektif sebagai mekanisme pengamanan tambahan dalam proses login.

Implementasi OTP yang dikirimkan melalui media komunikasi seperti aplikasi pesan instan menunjukkan bahwa mekanisme autentikasi dua faktor dapat diintegrasikan secara relatif mudah ke dalam sistem yang telah ada. Alur autentikasi yang diterapkan memastikan bahwa akses sistem hanya diberikan kepada pengguna yang berhasil melewati seluruh tahapan verifikasi, sehingga keamanan sistem dapat ditingkatkan secara signifikan tanpa mengubah struktur autentikasi utama secara menyeluruh. Meskipun demikian, penerapan OTP juga memiliki beberapa keterbatasan, antara lain penambahan langkah dalam proses login yang dapat memengaruhi kenyamanan pengguna, potensi pencurian OTP saat proses pengiriman, serta ketergantungan pada sinkronisasi waktu pada OTP berbasis waktu. Oleh karena itu, diperlukan perancangan sistem yang seimbang antara aspek keamanan dan kenyamanan pengguna agar penerapan 2FA dapat berjalan secara optimal.

Secara keseluruhan, penelitian ini menunjukkan bahwa penerapan autentikasi dua faktor berbasis OTP merupakan solusi yang efektif dalam meningkatkan keamanan akses sistem informasi. Penerapan 2FA direkomendasikan untuk sistem informasi akademik dan sistem lain yang menyimpan data sensitif sebagai upaya preventif dalam menghadapi ancaman keamanan siber. Penelitian selanjutnya diharapkan dapat mengembangkan metode autentikasi yang lebih aman, efisien, dan ramah pengguna, serta mengeksplorasi integrasi 2FA dengan teknologi keamanan lainnya.

REFERENSI

Ahmad Ilham Ali Mashudi, A. P. (2024). Rancang Bangun Sistem KeamananPintu Menggunakan Metode Two-Factor Authentication. *Journal of Informatics and Computer Science, 6*, 630-638.

Alfat Yanuar Fitriyansyah, M. (2020). AnalisisSecurity Web Login Mahasiswa Menggunakan Algoritma Two-Factor Time-Based One Time Password. *Vol. 30 No. 1 (2020): Jurnal Penelitian dan Pengkajian Sains dan Teknologi, 30*, 2-14.

Amry, Y., Ari , K., & Primantara , H. T. (Agustus 2025). IMPLEMENTASI TIME-BASED ONE-TIME PASSWORD MENGGUNAKAN ALGORITMA PHOTON UNTUK AUTENTIKASI DUA FAKTOR. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 12*, 799-808.

Daffa, S. I., & Joko, S. (2025). Designing a Two-Factor Authentication (2FA) System in E-Commerce Applications. *p–ISSN: 2723 –6609 e-ISSN: 2745-5254Vol. 6, 6*, 48-55.

Fajar Maulana, Y. H. (2025). Efektivitas dan Kelemahan Autentikasi Berbasis Web Menggunakan One-Time Password (OTP) dalam Mencegah Akses Tidak Sah. 682-690.

Ilham, G. A., Wina , W., & Herdi, A. (Februari 2025). Sistem Keamanan Otentikasi Pengguna pada Modul Single Sign On Menggunakan OAuth 2.0 dan One Time Password. *JURNAL ILMU KOMPUTER DAN TEKNOLOGI(IKOMTI), 6*, 25-31.

Iman, C., Husnul, M., Iwan, B., AndySutrisno, & Tofan, H. (September, 2024). EFFECTIVENESSOFMULTIFACTORAUTHENTICATION TECHNOLOGY FOR PROTECTING STUDENT PRIVACY:ASYSTEMATICLITERATUREREVIEW. *EdumJournal,Vol7,No2, 7*, 253-269.

Mahnida Zahra Siregar, N. F. (2024). PENERAPAN AUTENTIKASI DUA FAKTOR UNTUK KEAMANAN DATA PRIBADI DI INSTAGRAM. *Triwikrama: Jurnal Multidisiplin Ilmu Sosial, 6*.

Sari, A. P. (2025). Penerapan Autentikasi Dua Faktor (2FA) untuk Melindungi Data Pribadi pada Layanan Media Sosial. *JURNAL STARDIA, Volume 1, 1*, 60-65.

Yusuf , H., Anas , A. Q., & Iif , A. M. (2022). Pengembangan Metode Login Two Factor Authentication (2FA). *JINITA Vol. 4, No. 2, December 2022, 4*, 142-150.