# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Keamanan sistem informasi telah menjadi perhatian utama dalam perkembangan teknologi, terutama dalam konteks transaksi online dan aplikasi berbasis web yang memerlukan pertukaran data secara cepat dan aman. Salah satu teknologi yang sering digunakan dalam mengelola komunikasi antar sistem adalah *RESTful* API (Application Programming Interface). *RESTful* API memungkinkan pertukaran data yang mudah antar aplikasi dengan menggunakan protokol HTTP, namun rentan terhadap serangan jika tidak dilengkapi dengan pengamanan yang memadai (Satrio Utama & Dwi Indriyanti, 2023). Dalam beberapa kasus, kelemahan autentikasi pada RESTful API dapat dieksploitasi oleh pihak yang tidak berwenang, menyebabkan kebocoran data atau manipulasi transaksi (Purnama, 2018).

Menurut (Satrio Utama & Dwi Indriyanti, 2023) salah satu solusi yang sering diterapkan untuk mengamankan komunikasi dalam API adalah dengan menggunakan *JSON Web Token* (JWT). JWT merupakan standar token untuk mengamankan pertukaran data dengan cara mengenkripsi informasi yang dikirim antara klien dan *server*. Dengan JWT, hanya pengguna yang memiliki token yang dapat mengakses atau mengubah data yang dikirim melalui API. Algoritma yang digunakan untuk memastikan keamanan dalam JWT adalah HMAC-SHA512, algoritma ini memberikan proteksi kriptografis terhadap data yang dikirim melalui API.

Namun, meskipun penerapan JWT dapat meningkatkan keamanan, beberapa permasalahan autentikasi masih dapat terjadi. Salah satunya adalah kelemahan sistem yang hanya menggunakan *Single Factor Authentication* (SFA) dengan username dan password. Sistem SFA ini sangat rentan terhadap serangan *brute force*, di mana penyerang dapat mencoba berbagai kombinasi password untuk mendapatkan akses yang tidak sah (Setiawan et al., 2020).

PT. Kiosweb Teknologi Indonesia adalah penyedia jasa pembuatan aplikasi topup game dan PPOB (Payment Point Online Banking) berbasis web. Perusahaan ini didirikan dengan tujuan mempermudah akses bagi pengusaha pemula dan menengah yang ingin terjun ke dunia bisnis digital, terutama dalam penyediaan layanan top-up game dan produk PPOB. Hingga saat ini, Kiosweb telah membantu lebih dari 300 pelaku bisnis topup game di Indonesia, memfasilitasi mereka dengan aplikasi berbasis web yang mudah digunakan dan dilengkapi dengan berbagai fitur seperti transaksi otomatis 24 jam dan laporan penjualan yang terintegrasi secara real-time. Perusahaan ini juga menawarkan integrasi dengan berbagai vendor dan payment gateway seperti DigiFlazz, Apigames, Tokovoucher, Tripay, dan IPaymu, sehingga memudahkan proses top-up dan transaksi digital bagi penggunanya (Kiosweb, 2024b).

Berdasarkan hasil analisis studi kasus pada dokumentasi *hack* PT. Kiosweb Teknologi Indonesia, diketahui bahwa pada salah satu aplikasi topup game yang ada, sistem login hanya menggunakan username dan password sebagai autentikasi, tanpa ada keamanan tambahan seperti *Two-Factor Authentication* (2FA). Sehingga terjadi kerentanan ketika ada kebocoran data username dan password. Selain itu, ditemukan bahwa API order pada website bisa dilakukan duplikat *request* secara bersamaan. Hal ini mengakibatkan terjadinya *race condition*, di mana sistem gagal menangani permintaan simultan sehingga menyebabkan terjadinya transaksi yang tidak sah pada sistem. Akibatnya, saldo pengguna berkurang secara tidak sesuai dengan nominal transaksi, yang menyebabkan terjadinya kerugian pada perusahaan tersebut. Tidak adanya verifikasi *request* pada API order juga menjadi masalah, karena menyebabkan pengguna tidak sah untuk melakukan *request* tanpa autentikasi yang memadai (Kiosweb, 2024a).

Untuk mengatasi masalah-masalah tersebut, penerapan *Two-Factor Authentication* (2FA) berbasis *Time-Based One Time Password* (TOTP) adalah solusi yang dapat digunakan. TOTP merupakan algoritma yang menghasilkan kata sandi satu kali berdasarkan waktu dan *secret key* yang hanya berlaku untuk jangka waktu tertentu, sehingga memperkecil peluang terjadinya serangan

*replay attack* atau pencurian token (Ungkawa et al., 2017). Dengan penerapan TOTP, setiap permintaan melalui API akan memerlukan autentikasi tambahan, sehingga meningkatkan keamanan sistem secara keseluruhan.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengimplementasikan algoritma *Time-Based One Time Password* (TOTP) pada *Application Programming Interface* (API) guna meningkatkan keamanan autentikasi dan pertukaran data. Penelitian ini diharapkan dapat memberikan solusi yang efektif dalam menangani masalah autentikasi dan verifikasi *request* pada API yang digunakan untuk transaksi berbasis saldo. Adapun judul penelitian ini adalah **"PENGAMANAN *APPLICATION PROGRAMMING INTERFACE* DENGAN PENERAPAN *TWO-FACTOR AUTHENTICATION* MENGGUNAKAN ALGORITMA *TIME-BASED ONE TIME PASSWORD*"**.

## 1.2 Identifikasi Masalah

Berdasarkan uraian pada latar belakang masalah adapun identifikasi masalah yang dibahas adalah :

1. Sistem login pada aplikasi topup game berbasis web di PT. Kiosweb Teknologi Indonesia menggunakan *Single Factor Authentication* (SFA) yaitu username dan password sehingga terjadi kerentanan ketika ada kebocoran data username dan password.
2. API order pada aplikasi topup game berbasis web di PT. Kiosweb Teknologi Indonesia bisa dilakukan duplikat *request* secara bersamaan sehingga menyebabkan saldo berkurang tidak sesuai nominal transaksi.
3. Tidak ada verifikasi *request* pada API order sehingga menyebabkan *request* bisa dilakuan oleh pengguna yang tidak sah.

## 1.3 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan diatas, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana penerapan *JSON Web Token* (JWT) untuk API order pada aplikasi topup game berbasis web di PT. Kiosweb Teknologi Indonesia

dapat memberikan verifikasi *request* yang lebih aman dan mencegah pengguna tidak sah melakukan transaksi?

2. Bagaimana cara meningkatkan keamanan autentikasi login pada aplikasi topup game berbasis web di PT. Kiosweb Teknologi Indonesia yang hanya menggunakan username dan password dengan menerapkan *Two-Factor Authentication* (2FA) berbasis *Time-Based One Time Password* (TOTP)?
3. Bagaimana cara mencegah duplikat *request* pada API order untuk memastikan saldo berkurang sesuai dengan nominal transaksi dan mencegah kerugian pada sistem transaksi?

## 1.4 Batasan Masalah

Dalam pembahasan dan permasalahan yang diangkat, diperlukan pembatasan ruang lingkup atau batasan masalah agar penyajian menjadi lebih fokus dan saling berkaitan. Adapun batasan masalah tersebut adalah sebagai berikut:

1. Penelitian ini berfokus pada peningkatan keamanan *Application Programming Interface* (API) menggunakan *Two-Factor Authentication* (2FA) berbasis *Time-Based One Time Password* (TOTP).
2. TOTP digunakan sebagai otentikasi tambahan untuk memverifikasi setiap permintaan *request* yang dilakukan pada API order, dengan proses konfirmasi TOTP melalui email.
3. Penggunaan TOTP dengan *JSON Web Token* (JWT**)** sebagai mekanisme pengamanan tambahan untuk memastikan bahwa setiap *request* diverifikasi dan berasal dari pengguna yang sah.
4. Penelitian difokuskan pada pengembangan fitur-fitur inti yang digunakan dalam sistem transaksi, khususnya pada fitur berikut :
    - Fitur login yang digunakan ketika user akan mulai melakukan transaksi.
    - Fitur TOTP untuk menghasilkan kode TOTP sebagai autentikasi tambahan.
    - API profil untuk melakukan perubahan pada data user.
    - API order untuk proses transaksi atau pemesanan item.

- API produk untuk menampilkan daftar item.
- API metode pembayaran untuk menampilkan pilihan pembayaran.
- API deposit untuk melakukan deposit saldo.

5. Bahasa pemrograman yang digunakan PHP, MySQL, JavaScript, HTML, dan CSS.
6. Tools yang digunakan meliputi Draw.io untuk membuat UML dan alat bantu seperti Burp Suite, Postman serta Visual Studio Code untuk pengujian dan pembuatan API.
7. Fokus penelitian hanya mencakup verifikasi dan pengamanan pada *request* API untuk mencegah akses tidak sah dan manipulasi transaksi.

## 1.5 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah disampaikan, tujuan dari penelitian ini adalah :

1. Mengimplementasikan *Two-Factor Authentication* (2FA) berbasis *Time-Based One Time Password* (TOTP) untuk meningkatkan keamanan autentikasi login pada aplikasi berbasis web yang saat ini hanya menggunakan username dan password.
2. Mencegah duplikat *request* pada API order dengan penerapan otentikasi berbasis TOTP untuk memastikan saldo berkurang sesuai dengan nominal transaksi dan mencegah kerugian pada sistem transaksi.
3. Mengimplementasikan *JSON Web Token* (JWT) pada API order untuk memberikan verifikasi *request* yang lebih aman dan memastikan hanya pengguna yang sah yang dapat melakukan transaksi.

## 1.6 Manfaat Penelitian

Pada penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Manfaat Teoritis
   a. Penelitian ini diharapkan dapat mendukung dan menambah literatur yang ada mengenai penerapan *Two-Factor Authentication* (2FA) berbasis *Time-Based One Time Password* (TOTP) dalam meningkatkan keamanan autentikasi pada aplikasi berbasis web.

b. Memberikan pengetahuan, wawasan, informasi dalam pengembangan dan peningkatan keamanan pertukaran data serta autentikasi pada aplikasi berbasis web.

2. Manfaat Praktis:
   a. Bagi perusahaan, penelitian ini akan memberikan solusi dalam mengamankan proses login dan transaksi dari serangan seperti *race condition* dan akses tidak sah.
   b. Penelitian ini diharapkan membantu pengembang aplikasi untuk mengimplementasikan mekanisme pengamanan API yang lebih kuat, khususnya pada sistem transaksi dan sistem yang menggunakan API untuk pertukaran data.

   Pengguna akan mendapatkan jaminan keamanan lebih baik dengan adanya verifikasi tambahan pada saat login dan transaksi.

## 1.7 Pertanyaan Penelitian

Pertanyaan penelitian yang diajukan dalam penulisan proposal skripsi ini adalah sebagai berikut :

1. Bagaimana penerapan *JSON Web Token* (JWT) dapat meningkatkan keamanan dan verifikasi *request* API order pada aplikasi topup game berbasis web di PT. Kiosweb Teknologi Indonesia sehingga hanya pengguna yang sah yang dapat melakukan transaksi?
2. Bagaimana penerapan *Two-Factor Authentication* (2FA) berbasis *Time-Based One Time Password* (TOTP) dapat meningkatkan keamanan autentikasi login pada aplikasi topup game berbasis web di PT. Kiosweb Teknologi Indonesia, yang sebelumnya hanya menggunakan username dan password?
3. Bagaimana cara TOTP dapat mencegah duplikat *request* pada API order dan memastikan saldo berkurang sesuai dengan nominal transaksi?

## 1.8 Hipotesis Penelitian

Penerapan *Two-Factor Authentication* (2FA) berbasis *Time-Based One Time Password* (TOTP) dapat meningkatkan keamanan autentikasi login pada aplikasi berbasis web. Selain itu, penggunaan TOTP sebagai otentikasi

tambahan dapat mencegah duplikat *request* pada API order, sehingga memastikan saldo berkurang sesuai nominal transaksi. Implementasi *JSON Web Token* (JWT) juga meningkatkan keamanan dalam verifikasi *request* pada API order, mencegah akses dan transaksi oleh pengguna yang tidak sah.

## 1.9 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam penelitian ini mencakup beberapa metode, yaitu metode pengumpulan data, metode pengembangan system dan metode penyelesaian masalah. Berikut adalah pembahasan mengenai metode-metode tersebut :

### 1.9.1 Metode Pengumpulan Data

1. Studi Pustaka

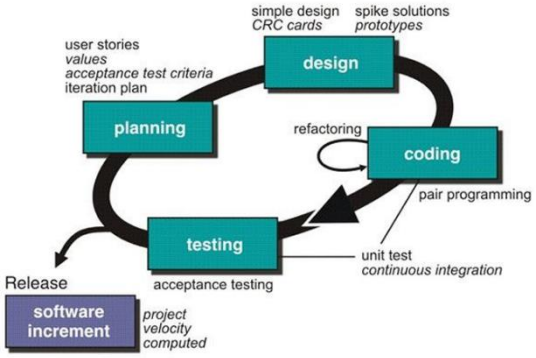
   Mengumpulkan referensi-referensi teori, kajian terkait penerapan *Two-Factor Authentication* (2FA)*, Time-Based One Time Password* (TOTP), dan *JSON Web Token* (JWT) dalam pengamanan *Application Programing Interface* (API) dan sistem transaksi.

2. Studi Kasus

   Menggunakan studi kasus di PT Kiosweb Teknologi Indonesia, di mana terjadi serangan *race condition* yang menyebabkan manipulasi saldo dalam sistem transaksi mereka

### 1.9.2 Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan dalam penelitian ini adalah metode Extreme Programming. Menurut (Borman et al., 2020), XP adalah metode dalam pengembangan perangkat lunak berbasis agile




*Gambar 1. 1 Fase Pada Extreme Programming (XP)*

yang berfokus pada pengkodean sebagai aktivitas utama dalam seluruh tahapan pengembangan. Metode ini responsif terhadap perubahan dan memungkinkan iterasi berulang untuk menyesuaikan kebutuhan sistem.

Adapun tahapan utama dalam XP meliputi:

1. *Planning* (Perencanaan)

   Tahap ini melibatkan pemahaman konteks bisnis, mendefinisikan fitur dan fungsi aplikasi, serta menyusun alur pengembangan sistem. Dalam hal ini peneliti melakukan pengumpulan data dengan cara studi pustaka terkait penerapan *Two-Factor Authentication* (2FA)*, Time-Based One Time Password* (TOTP), dan *JSON Web Token* (JWT) dalam pengamanan *Application Programing Interface* (API) dan sistem transaksi, serta melakukan analisis terhadap studi kasus di PT. Kiosweb Teknologi Indonesia.

2. *Design* (Perancangan)

   Pada tahap ini, focus pada desain aplikasi secara sederhana, alat untuk mendesain pada tahap ini misalnya dengan menggunakan CRC (Class Responsibility Collaborator) untuk memetakan kelas-kelas dalam diagram *use case diagram*, *class diagram* dan *activity diagram*. Pada tahap ini, saya melakukan perancangan sistem dengan menggunakan *Unified Modeling Language* (UML).

3. *Coding* (Pengkodean)

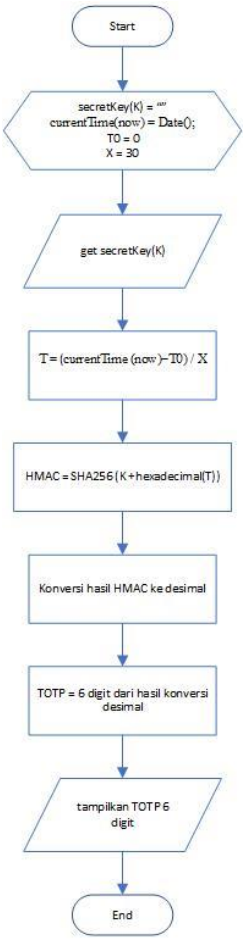
   Pengkodean merupakan proses penerjemahan desain ke dalam bahasa pemrograman yang dikenal oleh komputer. Pada tahap ini saya akan melakukan penerjemahkan bentuk desain ke dalam kode yang atau bentuk/bahasa yang dapat dibaca oleh mesin.

4. *Testing* (Pengujian)

   Tahap pengujian dilakukan untuk memastikan bahwa aplikasi berjalan sesuai kebutuhan, serta mendeteksi dan memperbaiki kesalahan yang ditemukan. Pada tahap ini saya akan melakukan pengujian sistem dengan menggunakan tools seperti burp suite dan postman.

### 1.9.3 Metode Penyelesaian Masalah

Time-Based One Time Password (TOTP) adalah algoritma yang dikembangkan dari HMAC (Hashes Message Authentication Code) yang menggabungkan antara *secret key* dengan current timestamp (waktu saat ini) dan menggunakan fungsi kriptografi hash untuk menghasilkan password sekali pemakaian (Ungkawa et al., 2017). Berikut adalah flowchart dan rumus pada algoritma TOTP.




*Gambar 1. 2 Flowchart Algoritma TOTP*

Proses untuk membuat password sekali pemakaian menggunakan algoritma Time-Based One Time Password (TOTP) ditunjukkan dengan persamaan sebagai berikut:

Dimana :

TOTP = HMAC(K, T)

T = currentTime (now) – T0/ X

HMAC = SHA256 (K + hexadecimal(T))

TOTP : *Time-Based One Time Password*.

HMAC: *Keyed-hash Authentication* sebuah fungsi *Code kriptografi* dikombinasikan dengan *secret key*.

K(Secret Key) : kode rahasia yang diambil dari serial number token virtual dan disimpan pada sisi server dan juga client.

T : jumlah time-steps antara inisialisasi counter T0 dan waktu saat ini.

currentTime : waktu saat ini (current time)

T0 : waktu awal inisialisasi, default diatur ke 0.

X : time-step yang umumnya diinisialisasi sebagai 30 detik.

## 1.10 Jadwal Penelitian

Jadwal kegiatan yang akan dilaksanakan dapat dilihat pada tabel berikut :

*Tabel 1. 1 Jadwal Penelitian*

| Tahapan | September | | | | Oktober | | | | November | | | | Desember - Maret | | | | April | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| Planning | | | | | | | | | | | | | | | | | | | | |
| Seminar Usulan Penelitian | | | | | | | | | | | | | | | | | | | | |
| Design | | | | | | | | | | | | | | | | | | | | |
| Coding | | | | | | | | | | | | | | | | | | | | |
| Testing | | | | | | | | | | | | | | | | | | | | |
| Seminar Hasil Penelitian | | | | | | | | | | | | | | | | | | | | |
| Skripsi | | | | | | | | | | | | | | | | | | | | |

## 1.11 Sistematika Penelitian

**BAB I : PENDAHULUAN**

Bab ini berisi latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan. Penjelasan mencakup alasan mengapa topik dipilih, masalah yang ingin diselesaikan, serta tujuan dan manfaat yang diharapkan dari penelitian ini.

**BAB II : LANDASAN TEORITIS**

Bab ini memuat teori-teori yang relevan sebagai dasar penelitian. Penjelasannya mencakup tinjauan pustaka, teori-teori yang mendukung solusi, dan kajian terhadap teknologi atau metode yang digunakan.

**BAB III : ANALISA DAN PERANCANGAN**

Bagian ini menjelaskan proses analisis masalah dan solusi yang dirancang. Penjelasan mencakup analisis kebutuhan, diagram perancangan (seperti diagram alur, ERD, atau DFD), serta metode yang digunakan untuk mengimplementasikan solusi.

**BAB IV : IMPLEMENTASI DAN PENGUJIAN**

Bab ini mendokumentasikan hasil implementasi dari rancangan pada BAB III, termasuk tampilan program atau sistem yang dihasilkan. Selain itu, dijelaskan pula proses pengujian, metode yang digunakan (seperti pengujian black-box atau white-box), dan hasil pengujian yang mencakup keberhasilan sistem dalam memenuhi kebutuhan.

**BAB V : KESIMPULAN DAN SARAN**

Bab ini memuat kesimpulan dari penelitian berdasarkan hasil implementasi dan pengujian. Selain itu, terdapat saran untuk pengembangan lebih lanjut atau untuk penelitian di masa depan, guna meningkatkan kualitas atau efisiensi dari solusi yang telah dibuat.