

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi harus mengoptimalkan pemanfaatan untuk pelayanan publik, salah satunya pada Kantor Pelayanan Perbendaharaan Negara [1]. Kantor Pelayanan Perbendaharaan Negara (KPPN) merupakan bidang pelayanan bendahara umum negara guna menyalurkan dana dari kas negara ke beberapa satuan kerja. KPPN bekerja di bawah direktorat jenderal perbendaharaan kementerian keuangan. Pada setiap provinsi terdapat beberapa perwakilan kantor KPPN yang bertanggung jawab untuk menyediakan layanan administrasi keuangan, informasi keuangan dan pelaporan keuangan setiap daerah kepada pemerintah pusat dan masyarakat. Salah satunya KPPN Yogyakarta merupakan instansi yang bergerak di bidang pelayanan keuangan milik negara di wilayah Yogyakarta . Perkembangan teknologi juga diterapkan pada layanan di kantor KPPN Yogyakarta, salah satu penerapan teknologi yaitu sistem layanan kerja berbasis *website* kppnjogja.id.

Website layanan kppnjogja.id merupakan aplikasi yang berguna untuk proses pengajuan dana keuangan kantor milik negara. Layanan kppnjogja.id digunakan oleh petugas administrasi untuk melakukan pendataan berkas-berkas yang akan menjadi syarat guna melakukan proses pencairan dana. Layanan kppnjogja.id tidak hanya dipakai oleh satu kantor, namun digunakan pada beberapa cabang kantor KPPN yang ada di provinsi Yogyakarta. Beberapa data operasional pengeluaran serta pencairan keuangan dari negara atau APBN serta terdapat data administrasi seperti pencairan gaji instansi kampus, TNI, Polri dan instansi lainnya milik negara. Data tersebut bersifat sensitif dan rahasia yang hanya diakses oleh pihak yang berwenang di KPPN memiliki hak akses atas layanan

kppnjogja.id. Data yang sensitif dan rahasia menjadi sangat rentan apabila terjadi manipulasi pencurian data oleh pihak-pihak yang tidak bertanggung jawab. Dengan ini dibutuhkan metode pengamanan data yang tersimpan di layanan kppnjogja.id guna mengurangi resiko kehilangan data [1].

Keamanan data pada sistem kppnjogja.id perlu ditingkatkan dengan menerapkan ilmu keamanan kriptografi. Kriptografi merupakan teknik enkripsi yang menggunakan kunci untuk mengubah teks biasa menjadi teks yang tidak dapat dibaca. Ini dapat dilakukan dengan menggunakan metode seperti penggeseran, substitusi, atau *hybrid* keduanya. Tujuan dari kriptografi adalah untuk menjaga informasi rahasia dan memastikan bahwa hanya orang yang memiliki kunci yang dapat mengakses informasi tersebut. *hybrid* metode dari kriptografi akan meningkatkan keamanan *Caesar Cipher* dan *Vigenere Cipher* merupakan salah satu metode yang termasuk kriptografi simetris. Pada *Vigenere Cipher* memiliki keunggulan kunci yang lebih panjang serta kunci yang tidak memiliki pola yang dapat diikuti oleh penyerang [2].

Pada *website* layanan kppnjogja.id masih adanya celah rentan untuk memanipulasi data, kerentanan diketahui melalui evaluasi keamanan *website* dengan menggunakan *tools OWASZAP*, menunjukkan terdapat 5 kerentanan keamanan yang sangat sensitif terutama pada *Cloud Metadata Potentially Exposed* yang dapat mengakibatkan tereksposnya data administrasi pada sistem layanan kppnjogja.id terutama data dokumen untuk melakukan pengajuan layanan . Oleh sebab itu yang menjadikan kelemahan keamanan pada layanan kppnjogja.id diperlukan untuk meningkatkan keamanan maka pada penelitian ini digunakan metode *Caesar Cipher* dan *Vigenere Cipher* untuk proses enkripsi dan dekripsi pada proses pengajuan layanan admistrasi yang terdapat pada sistem kppnjogja.id [3].

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dipaparkan, identifikasi masalah yang dapat ditemukan dari penelitian sebagai berikut :

1. KPPN Yogyakarta menggunakan sistem layanan kerja berbasis *website* (kppnjogja.id) untuk proses pengajuan dana keuangan. Sistem ini menjadi krusial dalam pengelolaan keuangan negara namun menyimpan berbagai data sensitif dan rahasia.
2. Risiko keamanan data dokumen pengajuan administrasi yang sensitif dan rahasia di layanan kppnjogja.id sangat rentan terhadap manipulasi dan pencurian oleh pihak yang tidak bertanggung jawab.
3. Kerentanan pada *website* dengan evaluasi keamanan menggunakan *tools PTES (Penetration Testing Execution Standard)* menunjukkan adanya kerentanan keamanan, terutama terkait dengan potensi terekposnya *Cloud Metadata*, yang menandakan adanya kelemahan dalam sistem keamanan *website* layanan kppnjogja.id.
4. Mengusulkan penggunaan metode *Caesar Cipher* dan *Vigenere Cipher* untuk proses enkripsi dan dekripsi dalam meningkatkan keamanan pada proses pengajuan layanan administrasi di sistem kppnjogja.id, yang memerlukan evaluasi terhadap efektivitas metode tersebut dalam mengatasi kerentanan yang ada.

1.3 Batasan Masalah

Batasan masalah yang diterapkan pada metode ini adalah :

1. Pengamanan data dokumen pada *database* yang dilakukan proses *hybrid* metode *Vigenere Cipher* dan *Caesar Cipher*.
2. Pengurangan potensi kerentanan keamanan dengan tingkat tinggi terutama pada *Cloud Metadata Potentially Exposed* yang dapat mengekspos data administrasi layanan.
3. Penggunaan *tools OWASP ZAP* dan *WIRESHARK* sebagai alat penguji dalam peningkatan keamanan pada *website kppnjogja.id*.

1.4 Rumusan Masalah

Sesuai dari identifikasi masalah yang telah dipaparkan di atas maka rumusan masalah yang akan dikaji adalah:

1. Bagaimana mengurangi tingkat kerentanan keamanan pada sistem layanan *kppnjogja.id*.
2. Bagaimana penerapan algoritma *vigenere cipher* dan *caesar cipher* guna meningkatkan keamanan pada aplikasi layanan berbasis web.
3. Bagaimana proses peningkatan keamanan dokumen pengajuan pada sistem layanan *kppnjogja.id*.
4. Bagaimana proses penggunaan *tools* guna pengujian tingkat keamanan sistem setelah diterapkan metode kriptografi.

1.5 Tujuan Penelitian

Adapun penelitian yang dilakukan memiliki beberapa tujuan sebagai berikut :

1. Menerapkan metode *Vigenere Cipher* dan algoritma *Caesar Cipher* untuk meningkatkan keamanan aplikasi berbasis web.
2. Mengurangi potensi kerentanan keamanan pada sistem layanan kppnjogja.id.
3. Meningkatkan keamanan *website* KPPN Yogyakarta.

1.6 Manfaat Penelitian

Manfaat yang dapat diperoleh dari hasil penelitian ini menjadi dua kategori utama, yaitu manfaat bagi mahasiswa yang melakukan penelitian dan bagi instansi KPPN Yogyakarta.

1. Manfaat Bagi Mahasiswa

- a. Peningkatan Pengetahuan dan Keterampilan mahasiswa dapat meningkatkan pemahaman terkait keamanan informasi, khususnya dalam konteks kriptografi, yang merupakan area penting dalam ilmu komputer dan teknologi informasi.
- b. Proses penelitian ini bermanfaat dalam membantu mahasiswa mengembangkan keterampilan penelitian, termasuk merancang studi, mengumpulkan dan menganalisis data, serta menyusun laporan penelitian yang komprehensif.
- c. Kontribusi Akademik Penelitian ini memberikan kontribusi kepada badan pengetahuan akademik, khususnya dalam bidang keamanan informasi dan kriptografi, yang dapat bermanfaat bagi penelitian masa depan.

2. Manfaat Bagi Instansi KPPN Yogyakarta
 - a. Peningkatan keamanan data melalui Implementasi metode enkripsi yang diusulkan oleh penelitian ini dapat meningkatkan keamanan data yang disimpan dan diproses oleh KPPN Yogyakarta, guna mengurangi risiko pencurian dan manipulasi data.
 - b. Peningkatan kepercayaan publik dengan memperkuat keamanan data dalam penggunaan sistem layanan kppnjogja.id
 - c. Menjaga keamanan data layanan agar tidak terekpos kepublik.