

ABSTRAK

PENGAMANAN DATA PENGGUNA PADA JSON WEB TOKEN (JWT) MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) UNTUK LAYANAN AUTENTIKASI

HARITS RAHMAN MAZAYAMUSTHAFA – 1157050066
Jurusan Teknik Informatika

Perkembangan teknologi informasi pada era saat ini telah mengalami kemajuan pesat dan sudah menjadi salah satu kebutuhan, baik dalam lingkup individu maupun organisasi. PT. Cerebrum Edukanesia Nusantara adalah perusahaan yang bergerak dibidang pendidikan yang memiliki berbagai fitur didalamnya. Masing-masing fitur memiliki sistem yang berbeda *platform* dan layanan. Penerapan REST API merupakan alternatif terbaik yang digunakan dalam mengatasi kondisi integrasi antar sistem dan pendistribusian data yang sedang dialami oleh pihak perusahaan. Untuk mengatasi kekurangan dari keamanan dan kebijakan hak akses tersebut, diperlukan layanan otentikasi untuk memberikan batasan hak akses data. JWT (JSON Web Token) merupakan sebuah *token* berbentuk *string* yang digunakan untuk melakukan otentikasi dan menjamin integritas pesan yang dikirim oleh salah satu pihak. Dibutuhkan keamanan data terhadap pertukaran data, maka perlu adanya metode kriptografi. Metode yang diimplementasikan adalah algoritma AES-128. Dengan adanya algoritma tersebut, diharapkan mampu membatasi penyalahgunaan oleh pihak yang tidak berhak mengetahui isi data yang telah dienkripsi tersebut, dan mengembalikan data yang dienkripsi tanpa mengalami perubahan data yang sesuai dengan data yang asli. Metode pengujian menggunakan *black box testing* dimana *black box testing* merupakan metode yang digunakan untuk menemukan kesalahan dan mendemonstrasikan fungsional sistem saat dioperasikan. Setelah melewati tahap pengujian pada implementasi REST API, maka dapat disimpulkan bahwa sistem keamanan data pengguna pada JWT menggunakan algoritma AES-128 telah berhasil dibangun.

Kata kunci: AES-128, API, JWT, REST, keamanan, distribusi data

ABSTRACT

SECURING USER DATA ON JSON WEB TOKEN (JWT) USING ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM FOR AUTENTICATION SERVICES

HARITS RAHMAN MAZAYAMUSTHAFA – 1157050066
Informatics Engineering

The development of information technology at this time has experienced very rapid progress and has become one of the needs of both individuals and organizations. Cerebrum Edukanesia Nusantara Company is a company engaged in education which has various features in it. Each feature has a different platform and service. The application of REST API is the best alternative used in overcoming the conditions of integration system and data distribution experienced by the company. To overcome the shortcomings of security and access right restrictions, the REST API is required for an authentication service to provide data access rights. JWT (JSON Web Token) is a string-shaped token that is used to authenticate and guarantee the integrity of messages sent by either party. Data security is needed for data exchange, so it is necessary to have a cryptographic method. The method implemented is the AES-128 algorithm. With this algorithm, it is hoped that it will be able to limit abuse by parties who are not entitled to know the contents of the encrypted data, and return the encrypted data without changing the data according to the original data. The test method uses black box testing where black box testing is a method used to find errors and demonstrate the functionality of the system when it is operated. After passing the testing phase of implementing the REST API, it can be concluded that the user data security system on JWT using the AES-128 algorithm has been successfully built.

Keywords: AES-128, API, JWT, REST, security, data distribution.