# ABSTRAK

Banyaknya angkutan umum yang beroperasi di Kabupaten Bandung menyebabkan repotnya pendataan secara manual. Proses pendataan yang masih manual menyebabkan banyaknya penggunaan kertas untuk mendata setiap angkutan umum. Penggunaan kertas yang terlalu banyak tersebut menyebabkan pemrosesan data seperti pencarian suatu data menjadi kurang efektif. Pada tugas akhir ini dirancang sebuah program RFID untuk pendataan angkutan umum secara digital (*paperless*).

Program RFID yang dirancang ini terhubung dengan *database* sistem informasi yang dikelola oleh Dinas Perhubungan Kabepaten Bandung, dan kemudian data tersebut diolah untuk dilakukan pendataan setiap angkutan umum. Program RFID ini menggunakan metode enkripsi data AES-128 (*Advanced Encryption Standard*) sebagai sistem keamanan data. Dalam penggunaan aplikasi, digunakan satu buah kunci privat yang hanya diketahui oleh petugas DISHUB. Dengan adanya sistem enkripsi data ini, pihak Dinas Perhubungan Kabupaten Bandung tidak lagi kerepotan untuk selalu memastikan keaslian data-data angkutan umum yang beroperasi dan bisa menjamin tidak ada pemalsuan data oleh pihak pemilik angkutan umum.

Hasil pengujian enkripsi AES pada kartu RFID menunjukkan performansi yang cukup baik. Waktu rata-rata enkripsi data pada 1 blok data adalah 0,273 detik, untuk dekripsi membutuhkan waktu yang sedikit lebih lama yaitu 0,305 detik pada tiap blok data. Untuk enkripsi dan dekripsi lebih dari blok data, waktu yang dibutuhkan sangat bergantung pada jumlah bloknya, semakin banyak blok yang diisi membuat waktu enkripsi dan dekripsi menjadi lebih lama. Kemudian pada pengujian *Avalanche Effect* menunjukkan nilai rata-rata yang cukup baik yaitu 47,5%. Untuk rasio keberhasilan validasi data ini adalah 100%, artinya aplikasi selalu menghasilkan nilai yang valid untuk enkripsi dan dekripsi.

**Kata Kunci :** RFID, enkripsi data, AES, keamanan data, angkutan umum

# ABSTRACT

Manual data collection process of public transportation in Bandung Regency leads to the use of many papers to record data and causes a search of a data becomes less effective. This paper design a digital data collection program (paperless) of RFID for public transportation and an encryption algorithm as a data security system. AES-128 algorithm is used to encrypt data.

This RFID program connected with the information system database managed by the Department of Transportation Bandung Regency, and then the data will be processed for data collection every public transportation. AES-128 use 1 private only officer knows. With the AES-128 encryption system, the Department of Transportation Bandung Regency no longer hassle to always make sure the public transportation data operation and can ensure there is no falsification of data by the owner of public transportation..

The results of AES Encryption on RFID card show the good performance of the system. Average time for encryption for 1 data block is 0.273s, for decryption need 0.305s for every block. Encryption and decryption time are depend on the number of block in use. Then the *Avalanche Effect* shows good value from average value 47.5%. Application has a success to give the valid data for encryption and decryption until 100%.



**Keywords :** RFID, data encryption, AES, data security, public transport