Multi-Factor Authentication Using a Smart Card and Fingerprint (Case Study: Parking Gate)

Isa Mulia Insan[1], Parman Sukarno[2], Rahmat Yasirandi[3]

School of Computing, Telkom University
Telekomunikasi Street Bandung (022) 7564108 Bandung, Indonesia

[1] muliainsan@student.telkomuniversity.ac.id
[2] psukarno@telkomuniversity.ac.id
[3] batanganhitam@telkomuniversity.ac.id

Abstract

Security is one of the considerations in the development of smart parking. In Indonesia, the most common authentication factor is using a smart card as an authentication factor at the gate. The use of smart cards as an authentication factor has loopholes that can be misused. Therefore an additional factor is needed for authentication. Authentication that uses more than one factor is also called Multi-Factor Authentication (MFA). However, MFA applied to smart parking can still be misused. The cause of the MFA can be misused is because the MFA cannot ensure the user's smart card. So, in this study applying the MFA at the gate in smart parking using a two-factor authentication system. These two factors are smart cards and biometric (fingerprint) data. This authentication system can solve problems where if the smart card is lost, the smart card can be used by other owners (P1), if the data smart card has been cloned, it can be a threat to the system (P2) and if the data is rewritten, it can become a threat to the system (P3). The ability of the system to overcome these problems is proven by passing several attack scenarios. Thus, the security of the proposed parking gate system can be guaranteed. Besides, the system has also passed a user agreement testing, in which the test results obtained by the proposed system experience an overhead time of 3.24s. However, the proposed system overhead time is still within the tolerance limit because the results of the proposed system safety comparison test have increased compared to the existing system.

Keywords: Multi-Factor Authentication, Smart parking, Smart card, Fingerprint, Biometric

Abstrak

Keamanan merupakan salah satu pertimbangan dalam pembangunan smart parking. Di Indonesia, faktor autentikasi yang paling banyak ditemui adalah menggunakan smart card sebagai faktor autentikasi pada gerbang. Penggunaan smart card saja sebagai faktor autentikasi memiliki celah yang dapat disalahgunakan. Maka dari itu dibutuhkan faktor tambahan untuk autentikasi. Autentikasi yang menggunakan lebih dari satu faktor disebut juga dengan Multi-Factor Authentication (MFA). Tetapi, MFA yang diterapkan pada smart parking masih dapat disalahgunakan. Penyebab MFA dapat disalahgunakan adalah karena MFA tersebut tidak dapat memastikan smart card user. Sehingga, pada penelitian ini menerapkan MFA pada gerbang di smart parking dengan menggunakan sistem autentikasi dua faktor. Dua faktor tersebut adalah smart card dan data biometric (fingerprint). Sistem autentikasi ini dapat mengatasi permasalahan yang mana apabila smart card hilang, smart card bisa digunakan oleh selain pemilik (P1), Apabila Smart card datanya telah cloning, dapat menjadi ancaman bagi sistem(P2) dan apabila Smart card datanya telah ditulis ulang, dapat menjadi ancaman bagi sistem(P3). Dapatnya sistem mengatasi permasalahan tersebut terbukti dengan melewati beberapa skenario serangan. Sehingga, keamanan sistem gerbang parkir yang diusulkan dapat dijamin. Selain itu sistem juga telah melewati user agreement testing, yang mana hasil pengujian yang didapat oleh sistem yang diusulkan mengalami waktu overhead sebesar 3.24s. Walaupun demikian, waktu overhead sistem yang diusulkan masih dalam batas toleransi karena, hasil dari pengujian perbandingan keamanan proposed system telah meningkat dibanding sistem yang ada.

Kata Kunci: Multi-Factor Authentication, Smart parking, Smart card, Fingerprint, Biometric